IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

LIBERTY PEAK VENTURES, LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
CITIGROUP INC. and CITIBANK, N.A.	§	**CIVIL ACTION NO. 6:21-cv-00710**
	§	
Defendants.	§	
	§	
	§	
	§	
	§	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Liberty Peak Ventures, LLC files this Complaint in this Western District of Texas (the "District") against Defendants Citigroup Inc. and Citibank, N.A. (collectively, "Defendants" or the "Citi Defendants") for infringement of U.S. Patent Nos. 7,953,671 (the "'671 patent"), 8,066,181 (the "'181 patent"), 8,794,509 (the "'509 patent"), 8,851,369 (the "'369 patent"), and 9,195,985 (the "'985 patent"), which are collectively referred to as the "Asserted Patents."

THE PARTIES

1. Plaintiff Liberty Peak Ventures, LLC ("LPV" or "Plaintiff") is a Texas limited liability company located at 1400 Preston Rd, Suite 482, Plano, TX 75093.

2. On information and belief, Defendant Citigroup Inc. ("Citigroup") is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 388 Greenwich Street, New York, NY 10013. Citigroup may be served with process via its

registered agents and via its corporate officers. Citigroup is a publicly traded company on the New York Stock Exchange under the symbol "C."

3. On information and belief, Defendant Citibank, National Association ("Citibank NA") is a national banking association regulated by the Securities and Exchange Commission and formed under the laws of Delaware. Citibank NA's principal executive office is located in 399 Park Avenue, New York, NY. Its principal place of business is 388 Greenwich Street, 14th floor, New York, N.Y. 10013. Citibank NA also has offices located at 5800 S Corporate Place, Sioux Falls, SD 57108. Citibank NA is an indirect, wholly-owned subsidiary of Defendant Citigroup. Citibank NA may be served with process via its registered agents and/or its corporate officers.

4. On information and belief, Defendant Citigroup "is a global diversified financial services holding company whose businesses provide consumers, corporations, governments and institutions with a broad, yet focused, range of financial products and services, including consumer banking and credit, corporate and investment banking, securities brokerage, trade and securities services and wealth management." *See 2020 Annual Report*, CITI, https://www.citigroup.com/citi/investor/quarterly/2021/ar20_en.pdf?ieNocache=293, at 26 ("Overview") (last downloaded June 11, 2021). Citigroup operates across the world having "200 million customer accounts and does business in more than 160 countries and jurisdictions." *Id*. Citigroup operates in four regions: 1) North America; 2) Europe, Middle East, and Africa; 3) Latin America; and 4) Asia. *Id*. at 26-7. The North American region consists of the U.S., Canada, and Puerto Rico. *Id*. Citigroup operates via two primary business segments consisting of a Global Consumer Banking (referred to also as "GCB") segment and an Institutional Clients Group segment. *Id*. The term "Citi" is used herein to refer to Defendant Citigroup, Inc. and all of its consolidated subsidiaries. *Id*.

5. On information and belief, Citibank NA "is a commercial bank and wholly owned subsidiary of Citigroup." *See id.* at 168. Citibank NA is one of Citigroup's "consolidated subsidiaries in which it holds, directly or indirectly, more than 50% of the voting rights or where it exercises control." *Id*. Citibank NA offers "consumer finance, mortgage lending and retail banking (including commercial banking) products and services; investment banking, cash management and trade finance; and private banking products and services." *Id*. These Citi products and services include Citibank NA offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing payment cards (e.g., credit card and debit cards) account services and transactions for Citi's customers, consumers, and clients. *See, e.g., Card Agreement*, CITI, https://www.citi.com/credit-cards/compare-credit-cards/citi.action?ID=CMA-PIT (indicating that "This Card Agreement…is your contract with us" and indicating that "us" means "Citibank, N.A.") (last visited June 11, 2021).

6. On information and belief, the Citi Defendants, individually and via their subsidiaries and affiliates, contract with and issue credit and debit cards to their customers ("cardholders") to provide card services. *See id.* The Asserted Patents cover Citi's products, services, and methods related to offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing commercial transactions via credit and debit cards and associated accounts, which are designed, developed, manufactured, distributed, sold, offered for sale, and used by the Citi Defendants and/or their customers, consumers, and clients. For example, within Citi's Global Consumer Banking segment, Defendants infringe the Asserted Patents via at least Citi's "Citi-branded cards," and "retail banking," which are services that allow Citi's clients and consumers to conduct financial and banking transactions via credit and debit cards, and their associated accounts. *See 2020 Annual Report*, at 27. Moreover, Defendants' infringing credit and

debit card account systems and processes are compatible with application ("app")-based mobile payment methods via third-party services, such as Google Pay, and Samsung Pay that are installed on a consumer's device, such as a mobile phone, tablet, or smartwatch. *See, e.g., Citi | G Pay, Show with east online and on the go*, CITI, https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-google-pay (last visited June 11, 2021).

7. On information and belief, Defendants, on their own and/or via subsidiaries and affiliates, maintain a corporate and commercial presence in the United States, including in Texas and this District, via at least its 1) physical bank locations, operation centers, and ATM locations established throughout Texas, including this District; 2) Citi's online presence (e.g., citi.com and citigroup.com) that provides to consumers access to Citi's products and services, including those identified as infringing herein; and 3) consumers and clients of Citi who utilize Citi credit and debit card account services, at the point of sale, including via contactless payment methods, in numerous merchant physical and online sites, i.e., retail stores, restaurants, and other service provides accepting Citi credit and debit cards. *See, e.g.*, *2020 Annual Report*, at 184 ("GCB includes a global, full-service consumer franchise delivering a wide array of banking, credit card, lending and investment services through a network of local branches, offices and electronic delivery systems."). Such credit and debit card account services include systems and methods for processing digital transactions, via online transactions and mobile payment solutions. *See, e.g., Consumer Business*, CITI, https://www.citigroup.com/citi/about/consumer_businesses.html ("With physical cards rapidly digitizing, we continued to expand digital lending capabilities and point-of-sale solutions to give customers ease, convenience and choice in payments."). Defendants, on their own and/or via alter egos, agents, subsidiaries, partners, and affiliates, maintain an operations center in this District located at 100 Citibank Dr, San Antonio, TX 78245, among other properties identified herein. Thus,

the Citi Defendants do business, including committing infringing acts, in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

8. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

A. Defendant Citigroup

10. On information and belief, Defendant Citigroup is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, partners, subsidiaries, clients, customers, affiliates, and/or consumers.

11. For example, Citigroup owns and/or controls multiple subsidiaries and affiliates, including, but not limited to Defendant Citibank NA that has a significant business presence in the U.S. and in Texas. *See, e.g.*, *Search & Apply for Jobs*, CITIGROUP.COM, https://jobs.citi.com/search-jobs?k=&l=&orgIds=287-34934 (Filter by "State" and "City" to see Citi employment locations across Texas, including Austin and San Antonio, soliciting 92 job openings) (last visited June 14,

2021). Citigroup, via its own activities and via at least wholly owned subsidiary Citibank NA, has an operations center in San Antonio, TX, among other properties, in this District, at 100 Citibank Dr, San Antonio, TX 78245. *See Shape your Career with Citi in San Antonio, Texas*, CITIGROUP.COM, https://jobs.citi.com/sanantonio ("We are extremely proud to be the home away from home for 2,400 talented, dedicated, and inspiring people at various stages of life.") (last visited June 14, 2021). Bexar county CAD search results show that Defendant Citibank NA's subsidiary Citicorp Credit Services Inc. (USA) ("Citicorp Credit") is the listed owner of Citigroup's San Antonio operations center, which is a campus comprising at least four separate structures. *See Property Search Results > 1 - 24 of 24 for Year 2021*, BEXAR CAD, http://bexar.trueautomation.com/clientdb/SearchResults.aspx?cid=110 (under advanced property search type "citi") (last visited June 14, 2021). Citicorp Credit is registered to do business in Texas and is 100% owned by Citibank NA. Citigroup's operations center employs over two thousand (2,000) residents of the state of Texas and this District. *See CITI HOSTS SEPTEMBER BOARD OF DIRECTORS MEETING*, SAN ANTONIO CHAMBER OF COMMERCE, Sept. 27, 2019, https://www.sachamber.org/news/2019/09/27/board-action-report-september-2019/ ("Citi employs 2,500 employees locally and has an established reputation for being military friendly, embracing an inclusive office culture, and championing healthy work-life balance. Citi demonstrates its commitment to the community through corporate giving campaigns and employee volunteer partnerships with more than 20 organizations, and last year Citi employees dedicated more than 10,000 hours to volunteer efforts.") (last visited June 14, 2021).

12. Other subsidiaries of Defendants, including Citifinancial Inc. and Citimortgage Inc., are listed owners of residential properties in Bexar county. Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. are each registered to do business in Texas.

13. Such a corporate and commercial presence in Texas, including in this District, by Defendant Citigroup furthers the development, design, manufacture, distribution, sale, and use of Citigroup's infringing products, services, and methods for offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing commercial transactions via credit and debit cards and associated accounts. Through direction and control of its alter egos, intermediaries, agents, subsidiaries and affiliates, Citigroup has committed acts of direct and/or indirect patent infringement within Texas, this District, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Citigroup would not offend traditional notions of fair play and substantial justice.

14. On information and belief, Citigroup controls or otherwise directs and authorizes all activities of its alter egos, intermediaries, agents, subsidiaries, and affiliates, including, but not limited to Defendant Citibank NA and other subsidiaries Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. Via its own activities and via at least these entities, Citigroup has substantial business operations in Texas, which include retail and non-profit partners, clients, customers and related financial products and services, such as retail banking services, investment services, Citi-branded cards, and private label and co-brand cards. Citigroup has placed and continues to place infringing products, services, and methods for offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing commercial transactions via credit and debit cards and associated accounts, including related mobile, contactless, and online payment systems, into the U.S. stream of commerce. Citigroup has placed such products, services, and methods into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or used in this District and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523

F.3d 1353, 1369-70 (Fed. Cir. 2008) ("[T]he sale [for purposes of § 271] occurred at the location of the buyer.").

15. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Citigroup has committed acts of infringement in this District. As further alleged herein, Defendant Citigroup, via its own operations and employees located there and via ratification of Defendant Citibank NA's presence and the presence of other subsidiaries as agents and/or alter egos of Citigroup, has a regular and established place of business, in this District at least at an operations center located at 100 Citibank Dr, San Antonio, TX 78245. Accordingly, Citigroup may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant Citibank NA

16. On information and belief, Defendant Citibank NA is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, Citibank NA, including as an agent and alter ego of parent company Citigroup, owns a Citi operations center in San Antonio, TX, via its subsidiary Citicorp Credit Services Inc. (USA), that employs over 2,000 Citi employees, operates a large network of Citibank ATMs, and maintains in a retail services and

retail banking business that provides to products, services, and methods that include Citibank NA offering, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card account services, via credit and debit cards and associated accounts, including related mobile, contactless, and online payment systems, for Citi's customers, consumers, and clients in Texas and this District. Moreover, Citibank NA identifies itself as the Citi entity that issues Citi credit and debit cards to Citi's clients, consumers, and customers. *See, e.g.*, *Card Agreement*, CITI, *available at* https://www.citi.com/CRD/PDF/CMA/cardAgreement/CMA_PID410.pdf ("This Card Agreement (Agreement) is your contract with us," and, under Definitions, "we, us and our – Citibank, N.A.") (last visited June 17, 2021).

17. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). Defendant Citibank NA has committed acts of infringement in this District. As further alleged herein, Defendant Citibank NA, via its own operations and employees located there and via ratification of its subsidiary Citicorp Credit Services Inc. (USA)'s presence and the presence of other subsidiaries as agents and/or alter egos of Citibank NA, has a regular and established place of business, in this District at least at an operations center located at 100 Citibank Dr, San Antonio, TX 78245. Accordingly, Citibank NA may be sued in this district under 28 U.S.C. § 1400(b).

18. On information and belief, Defendants Citigroup and Citibank NA each have significant ties to, and presence in, the State of Texas and this District, making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

19. The Asserted Patents cover various aspects of products, services, and methods that include the Citi Defendants' offering, issuing, providing, registering, facilitating, maintaining,

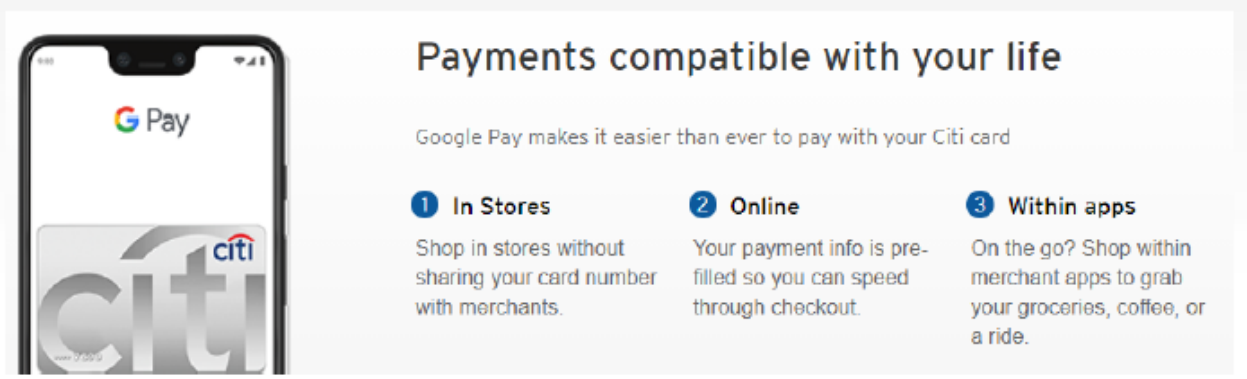
transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi's customers, consumers, and clients, including Citi's internal payment processing, authentication, authorization, and fraud detection systems and methods, referred to herein collectively as the "Accused Instrumentalities." The apparatuses, systems, and methods described in each of the Asserted Patents apply, for example, to systems for securing, authorizing, and facilitating financial transactions, i.e., purchases, related to credit and debit card accounts.

20. On information and belief, a significant portion of the operating revenue of the Citi Defendants is derived from offering and selling products, services, and methods related to issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts, and related financial benefits of, including fees and interest, for Citi's customers, consumers, and clients. Citi's North America revenues in 2020 were $19.1 billion U.S. dollars; this included Citi-branded card revenues of $8.8 billion U.S. dollars. *See 2020 Annual Report*, at 7.

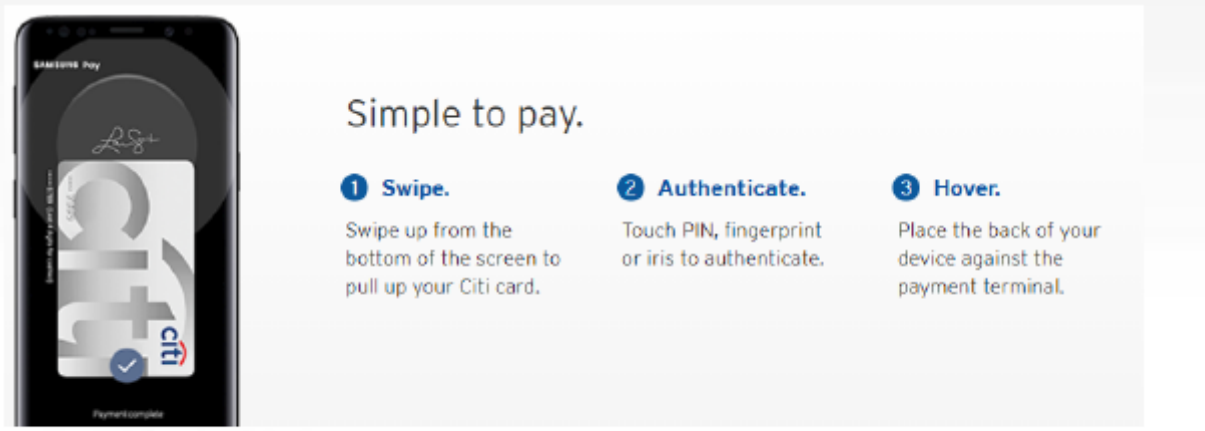
21. The Asserted Patents cover Accused Instrumentalities of the Citi Defendants that secure, authorize, and facilitate mobile payments, contactless payments, and online payments using credit and debit card accounts activated, offered, issued, provided, established, registered, facilitated, and maintained by Citi, including by the Citi Defendants and their alter egos, intermediaries, agents, distributors, partners, subsidiaries, and clients. Clients, customers, and consumers of the Accused Instrumentalities use such products at the point of sale, for example, via mobile wallets provided on a mobile device with the appropriate smartcard and/or app installed (and in some cases the software is native to the device) or via an embedded chip or smartcard embedded within a physical credit or debit card. In other instances, the Accused Instrumentalities

may be utilized in online purchases conducted over a network (e.g., the Internet) and/or when the user of the payment card account is registering, activating, or maintaining the account.

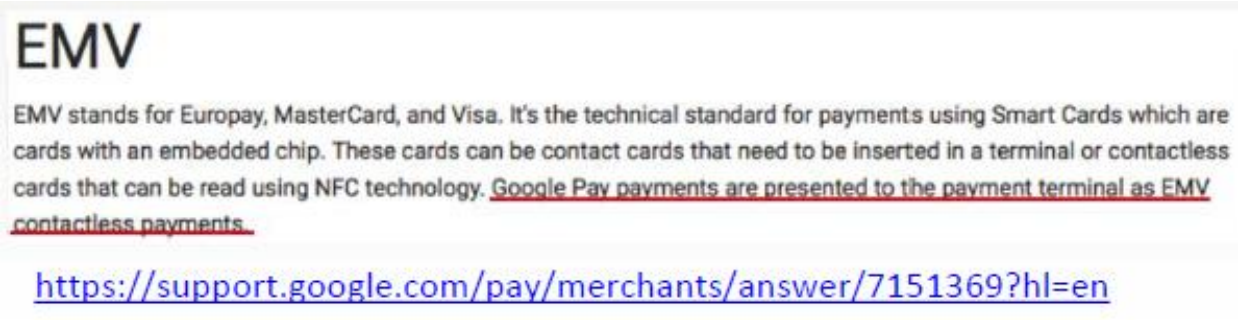
22. On information and belief, Citi's credit and debit card account services utilize the Europay, Mastercard, and Visa (EMV) standards in processing, securing, and authenticating financial transactions. For example, the Citi Defendants provide payment applications (often provisioned to a Secure Element) that use EMV standards to process payments. In some cases, the Citi Defendants' payment applications reside on a user's mobile device (e.g., stored in a Secure Element or other secure memory), allowing the user to make payments via a Citi credit or debit card without presenting the physical card at the time of payment (referred to herein as a "mobile payment"). Citi's mobile payments can be facilitated by using mobile wallets such as Google Pay and Samsung Pay, such as shown below:

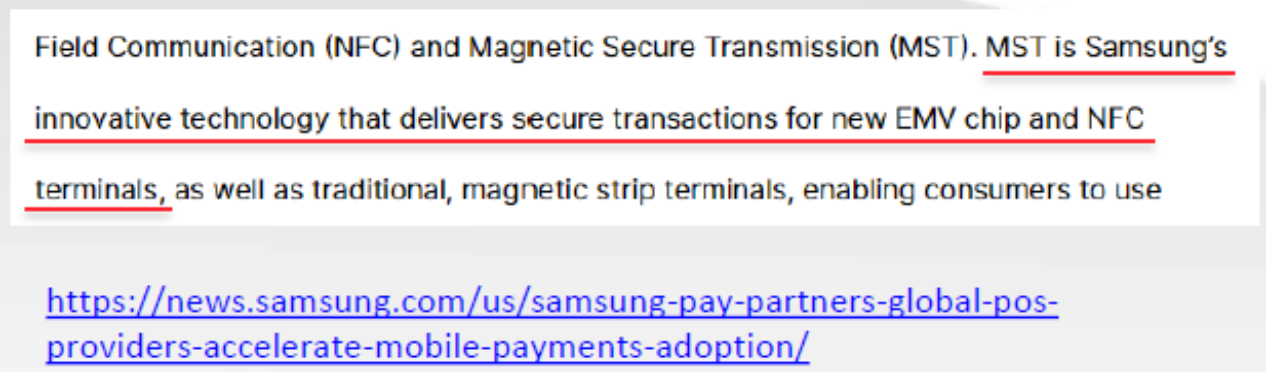


https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-google-pay



23. Mobile wallets may be implemented as an application (or "app") on a mobile device, e.g., a mobile phone, tablet, or smartwatch. In some implementations, mobile wallets utilize Host Card Emulation, where, instead of storing the Citi's payment application in a Secure Element on the host device, it is stored in the host CPU or remotely, e.g., in the cloud. In either case, mobile payments are made wirelessly, without contact needed between payment device and payment terminal, via, for example, Near Field Communication ("NFC") protocols or Magnetic Secure Transmission (MST), as explained below. A user need only hold the mobile device close to the payment terminal in order to establish communication between the payment application and the payment terminal. These wireless methods utilized with EMV deliver secure transactions between a payment terminal and the mobile device.




Field Communication (NFC) and Magnetic Secure Transmission (MST). MST is Samsung's innovative technology that delivers secure transactions for new EMV chip and NFC terminals, as well as traditional, magnetic strip terminals, enabling consumers to use

https://news.samsung.com/us/samsung-pay-partners-global-pos-providers-accelerate-mobile-payments-adoption/

24. On information and belief, as indicated below, Citi encourages its clients, consumers, and customers to shop with its Citi credit and debit cards using a digital wallet service which provides a distribution channel by which Citi's payment applications (e.g., via the Secure Element on the mobile device) can be accessed and used:

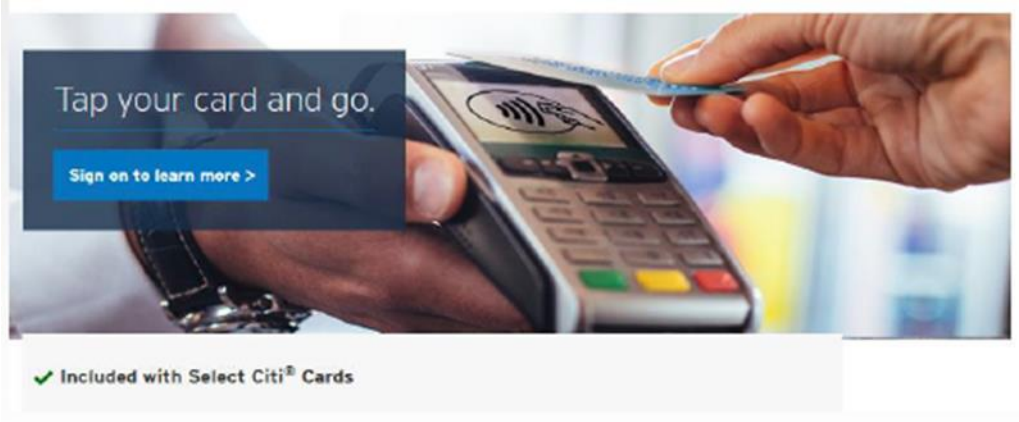
Here is how you can use digital wallets:

- **For online shopping**: Digital wallet services like Masterpass™ allow you to store details like your payment information and shipping address in a centralized account so that you don't have to enter all of your information every time you shop online – just look for your digital wallet as a payment option when checking out at your favorite merchants, sign in using your username and password, and then complete your purchase.
- **Within an app**: These are typically retailer-specific apps connected to your payment information– and can be used for everything from pre-ordering your morning coffee to paying for it and collecting loyalty points. Many also allow you to store rewards and coupons as digital barcodes, which can then be scanned when you're at the cash register to get a discount on your purchase.
- **In the store**: Here, you don't need to swipe a card, enter a PIN at the register, or sign a receipt; you simply tap your smartphone on a contactless-enabled terminal, usually located near the register at check-out. After you tap, an additional step (or steps, depending on your device) is usually required to complete the transaction, such as fingerprint authentication or entering a passcode into your mobile phone.

See Digital Wallets Demystified, CITI, https://www.citi.com/credit-cards/credit-card-rewards/digital-wallets-and-virtual-wallets (last visited June 15, 2021).

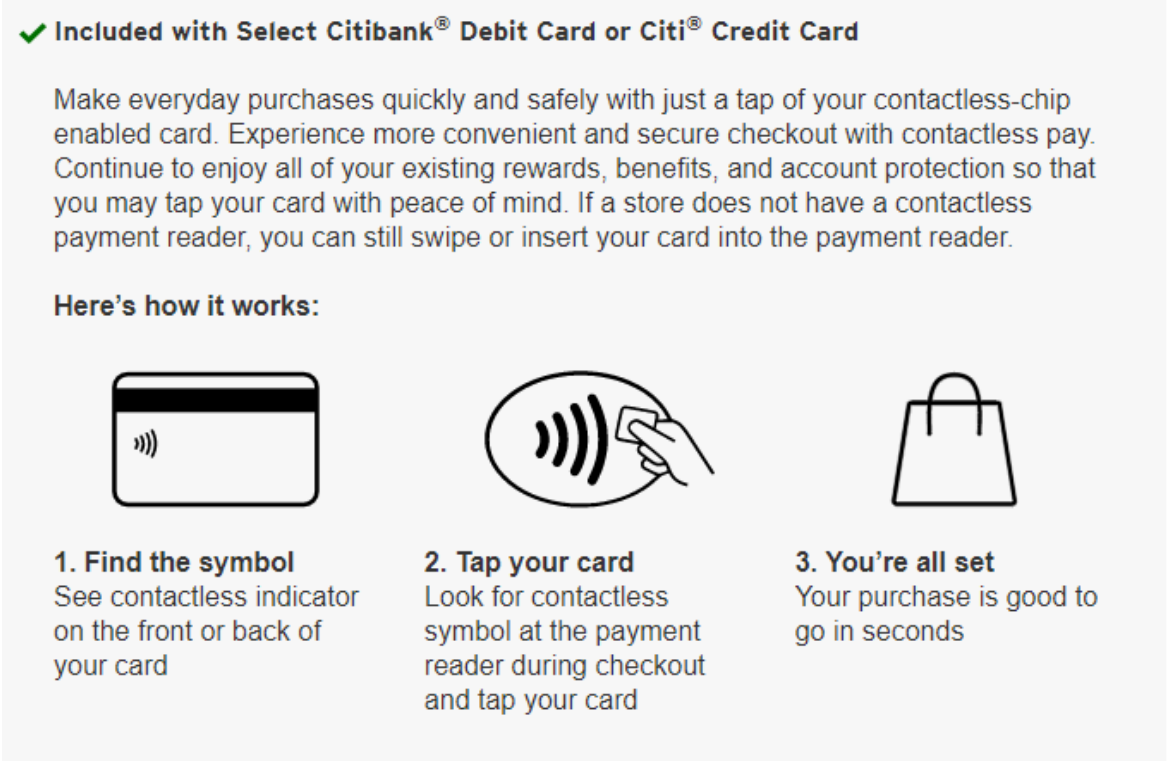
25. The Accused Instrumentalities also include at least Defendants' payment card (e.g., credit card and debit card) related products, services, and methods for card payments using a physical credit card having an embedded chip or smartcard. *See, e.g., View and Compare All Credit Cards*, CITI, https://www.citi.com/credit-cards/compare/view-all-credit-cards (last visited June 15, 2021). For example, the Citi Defendants' payment applications reside on microchips embedded on

Citi's credit and debit cards, which allow the user to tap the payment card to a reader and complete a transaction wirelessly and without contact between the card's magnetic stripe and the reader.



https://www.cardbenefits.citi.com/Products/Contactless-Card?cmp=PAC~00~190214~BENBUILD~contactless

26. On information and belief, the Accused Instrumentalities include at least Defendants' payment card (e.g., credit card and debit card) related products, services, and methods for contactless payments using a physical credit card having an embedded chip or smartcard that utilize EMV standards for contactless payment. *See, e.g., View and Compare All Credit Cards*, CITI, https://www.citi.com/credit-cards/compare/view-all-credit-cards (last visited June 15, 2021). These credit and debit cards include contactless payment functionality indicted by the signal symbol, and further described below.



See Citi Credit Card Benefits, CITI, https://www.cardbenefits.citi.com/Products/Contactless-Card (last visited June 15, 2021).

27. On information and belief, a process referred to as "tokenization," which is also part of the EMV standards, is also utilized by the Citi Defendants in authorizing credit and debit transactions, via online payments, in-app payments, and mobile payments. As explained below, a "payment token" is a "surrogate value for a PAN" (a primary account number). In tokenization, "Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs." *See also Introducing Tokenization*, CITI, https://www.citibank.com/tts/sa/commercial_cards/newsletter/2016_Q3/tokenization.html ("Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, which has no extrinsic or exploitable meaning or value.") (last visited June 18, 2021).

Payment Token	A surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric issued from a designated Token BIN or Token BIN Range and flagged accordingly in all appropriate BIN tables. A Payment Token must pass basic validation rules of a PAN, including the Luhn check digit. Payment Tokens must not collide or conflict with a PAN.
Payment Tokenisation	A specific form of tokenisation whereby Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs as described by the processes defined in this technical framework.

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0.pdf

28. Via mobile wallet applications, such as Google Pay, tokenization is implemented by the Citi Defendants assigning a "virtual account number" or token that "securely links the actual card number to a virtual card on the user's Google Pay-enabled device."

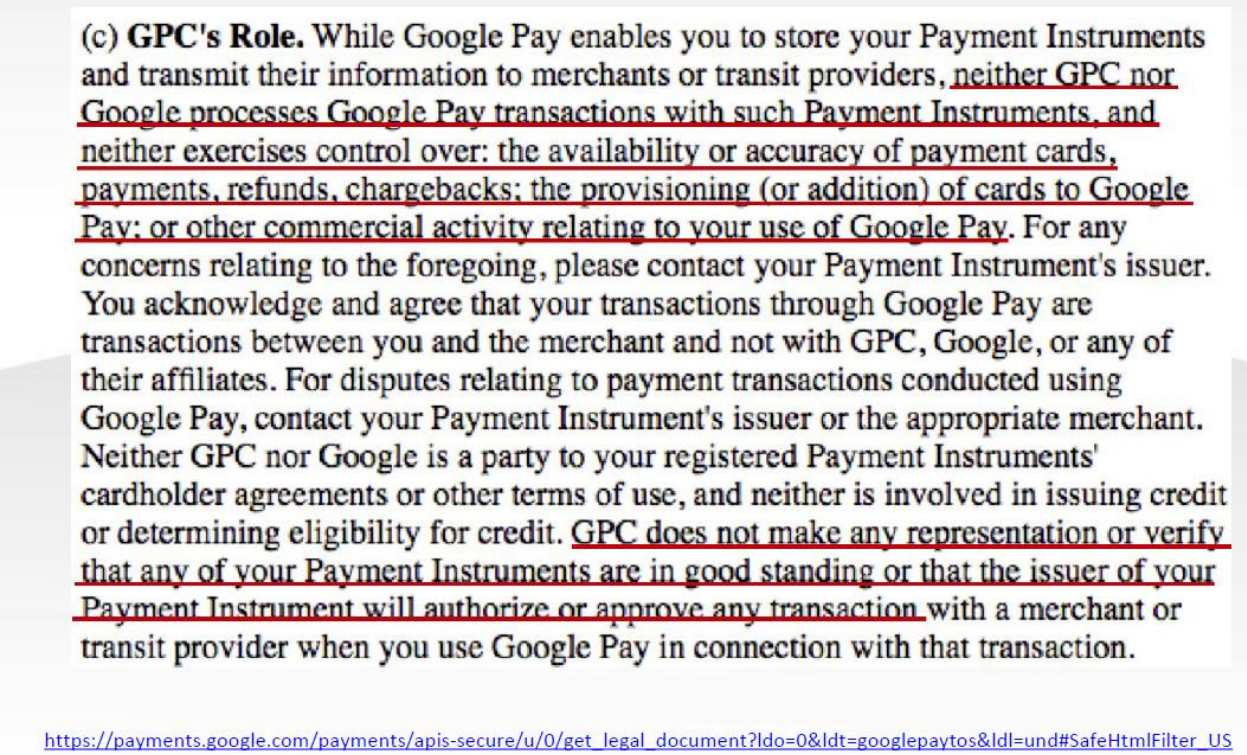
Tokenization

Google Pay facilitates the assignment of a "virtual account number," also called a token, that securely links the actual card number to a virtual card on the user's Google Pay-enabled device. A token is unique to the card number it represents. The app user's mobile device keeps an encryption key in memory that it uses to decrypt limited-use and single-use keys (also called cryptograms) for contactless transactions (NFC payments).

https://support.google.com/pay/merchants/answer/7151299?hl=en

29. The Citi Defendants, as a payment card account issuer, direct and control the operation of mobile wallets and contactless payments utilizing microchips or smartcards embedded within the physical credit or debit card. As described below with respect to the mobile wallet Google

Pay, for example, the Citi Defendants provision third-party mobile wallets with the Citi Defendants' own credentials and EMV payment applications.



(c) **GPC's Role.** While Google Pay enables you to store your Payment Instruments and transmit their information to merchants or transit providers, neither GPC nor Google processes Google Pay transactions with such Payment Instruments, and neither exercises control over: the availability or accuracy of payment cards, payments, refunds, chargebacks; the provisioning (or addition) of cards to Google Pay; or other commercial activity relating to your use of Google Pay. For any concerns relating to the foregoing, please contact your Payment Instrument's issuer. You acknowledge and agree that your transactions through Google Pay are transactions between you and the merchant and not with GPC, Google, or any of their affiliates. For disputes relating to payment transactions conducted using Google Pay, contact your Payment Instrument's issuer or the appropriate merchant. Neither GPC nor Google is a party to your registered Payment Instruments' cardholder agreements or other terms of use, and neither is involved in issuing credit or determining eligibility for credit. GPC does not make any representation or verify that any of your Payment Instruments are in good standing or that the issuer of your Payment Instrument will authorize or approve any transaction with a merchant or transit provider when you use Google Pay in connection with that transaction.

https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=googlepaytos&ldl=und#SafeHtmlFilter_US

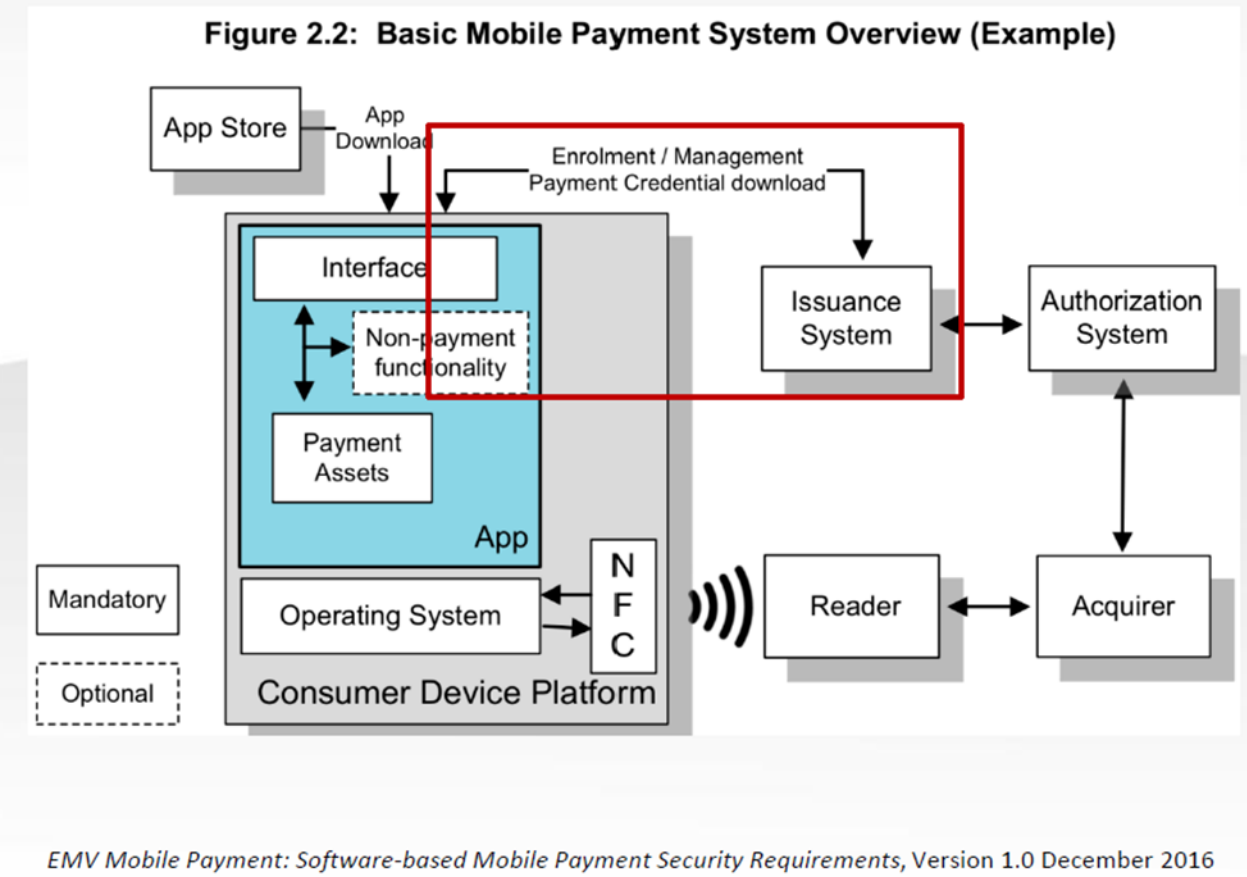
30. The Accused Instrumentalities include Citi's products, processes, and systems offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi's customers, consumers, and clients, including Citi's internal payment processing, authentication, authorization, and fraud detection systems and methods, related to at least the following Citi payment cards: Citi Custom CashSM Card; Citi® Diamond Preferred® Credit Card; Citi® Double Cash Credit Card; Citi Rewards+® Credit Card; Citi Premier® Credit Card; Citi Prestige® Credit Card; Citi® Secured Mastercard® Credit Card; Citi Simplicity® Credit Card; Citi® / AAdvantage® Platinum Select® World Elite Mastercard® Credit Card; American Airlines AAdvantage® MileUpSM Mastercard® Credit Card; Citi® / AAdvantage® Executive World Elite Mastercard® Credit Card; CitiBusiness® / AAdvantage® Platinum Select® Mastercard® Credit

Card; Shop Your Way Mastercard; Sears Mastercard; Sears Mastercard with Thank You Rewards; Exxon Mobile Smart Card; Costco Anywhere Visa® Credit Card by Citi; Costco Anywhere Visa® Business Credit Card by Citi; Expedia® Rewards Credit Card from Citi; Expedia® Rewards Voyager Credit Card from Citi; AT&T Access Credit Card From Citi; Citi Wayfair MasterCard; MY BEST BUY® VISA® PLATINUM; Brooks Brothers Platinum Mastercard; Home Depot Commercial Revolving Charge Card; Home Depot Commercial Account; Home Depot Consumer Credit Card; Shell Fuel Rewards Mastercard; and Citibank® Debit Card. *See, e.g.*, *Payments compatible with your life*, CITI, https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-google-pay ("All Citi branded consumer credit and debit cards issued in the US are eligible for Google Pay, except for ATM cards, American Express cards, and Citi® / AAdvantage® cards. Citi branded business cards are not eligible for Google Pay, except for US issued Costco Anywhere Visa® Business cards.") (last visited June 17, 2021).

31. The Accused Instrumentalities of the Citi Defendants infringe at least claims of the '671 patent, which provide technological solutions and improvements addressing security concerns surrounding the provisioning of credentials to, and transactions performed using, digital wallets. Though conventional methods for securing financial transactions utilized use of personal identifiers, such as PINs, such identifiers could be easily duplicated or discovered. Even with the use of electronic wallets and more intelligent instruments, there remained a need to further safeguard electronic transactions against evolving threats. In at least one exemplary embodiment, the '671 patent addresses the need for securing RFID transactions by establishing a challenge from a computer-based system sent to an intelligent token of a client. The token generates a challenge response that is received by the computer-based system. Credentials, assembled by the computer-based system, include a key. In a given transaction, a client may make a request to the computer-

based system including at least a portion of the assembled credentials. The computer-based system may validate the portion of the assembled credentials with the key, and provide access to a transaction service. Utilizing systems and methods such as these, the '671 patent's claims allow payment card issuers to secure direct and safe transactions between consumers and merchants.

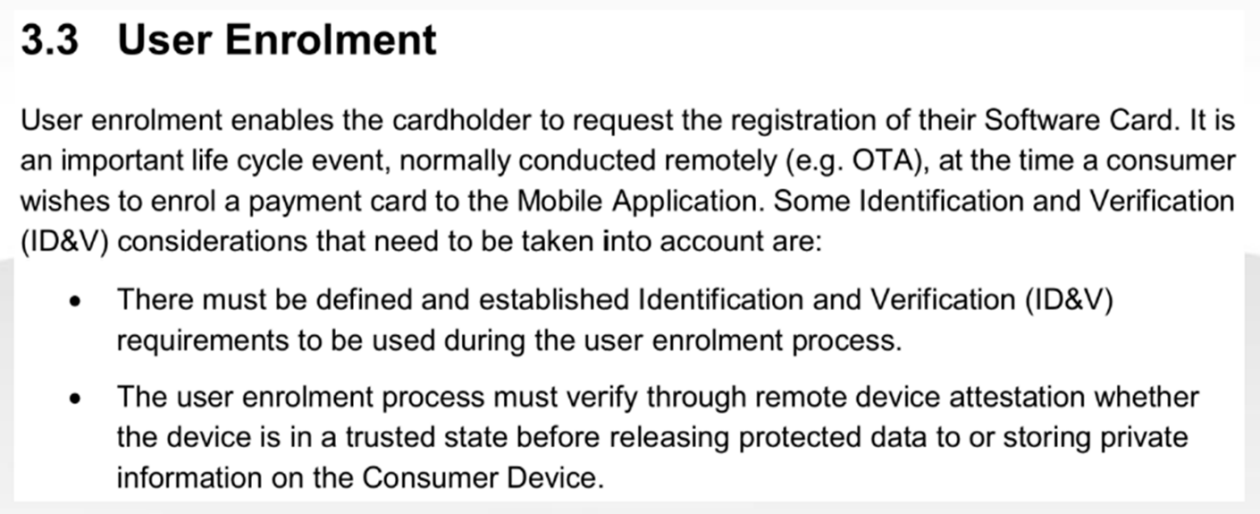
32. The Citi Defendants infringe the '671 patent by enabling and conducting mobile payments that utilize mobile wallets, such as Google Pay and Samsung Pay. These mobile wallets conform to EMV standards. As part of utilizing a consumer's mobile wallet, the Citi Defendants conduct an enrollment process, which forwards a challenge to a consumer's mobile device, i.e., an intelligent token, as shown below.



EMV Mobile Payment: Software-based Mobile Payment Security Requirements, Version 1.0 December 2016

33. As described below, the challenge is used in the enrollment process for identification and verification of the consumer, as a user of the mobile wallet, and for device

attestation to determine that the device is in a trusted state. Furthermore, the Citi Defendants receive this challenge response.



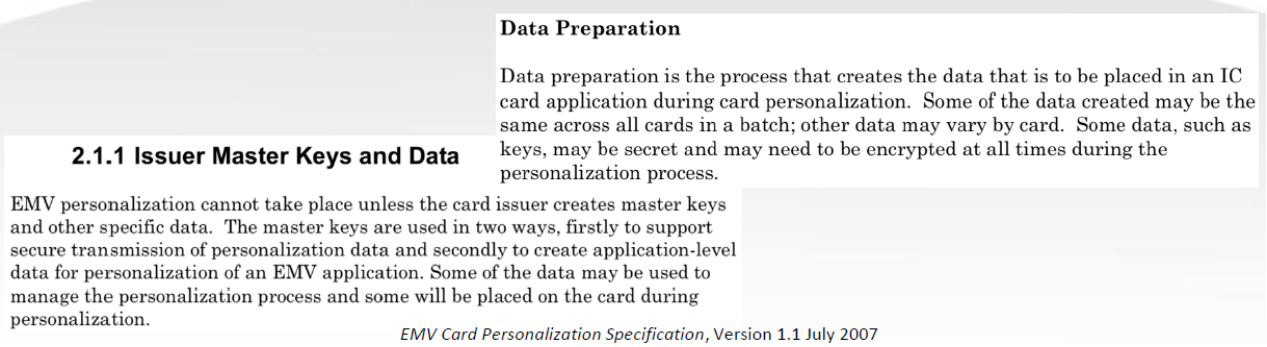
3.3 User Enrolment

User enrolment enables the cardholder to request the registration of their Software Card. It is an important life cycle event, normally conducted remotely (e.g. OTA), at the time a consumer wishes to enrol a payment card to the Mobile Application. Some Identification and Verification (ID&V) considerations that need to be taken into account are:

- There must be defined and established Identification and Verification (ID&V) requirements to be used during the user enrolment process.
- The user enrolment process must verify through remote device attestation whether the device is in a trusted state before releasing protected data to or storing private information on the Consumer Device.

EMV Mobile Payment: Software-based Mobile Payment Security Requirements, Version 1.0 December 2016

34. The Citi Defendants further assemble credentials, including encryption keys, to be used when effecting transactions, referred to as "provisioning" below.



Data Preparation

Data preparation is the process that creates the data that is to be placed in an IC card application during card personalization. Some of the data created may be the same across all cards in a batch; other data may vary by card. Some data, such as keys, may be secret and may need to be encrypted at all times during the personalization process.

2.1.1 Issuer Master Keys and Data

EMV personalization cannot take place unless the card issuer creates master keys and other specific data. The master keys are used in two ways, firstly to support secure transmission of personalization data and secondly to create application-level data for personalization of an EMV application. Some of the data may be used to manage the personalization process and some will be placed on the card during personalization.

EMV Card Personalization Specification, Version 1.1 July 2007

35. In a given transaction, the Citi Defendants receive a request from the consumer's mobile wallet, which include the assembled credentials, such as the application primary account number (PAN or also token) and an Application Cryptogram, which is encrypted with the provided

key. As described below, the Citi Defendants validate the consumer's credentials using the provided key.

Table 10 contains existing data elements necessary for an ICC transaction.

Data Element	Condition
Acquirer Identifier	Present for Terminal Type = '1x' or '2x' if Merchant Identifier or Terminal Identifier does not implicitly refer to a single acquirer
Amount, Authorised * [12]	
Amount, Other *	Present if cashback used for current transaction
Application Effective Date	Present if in ICC
Application Expiration Date	Present if not in Track 2 Equivalent Data
Application PAN *	Present if not in Track 2 Equivalent Data
Application PAN Sequence Number *	Present if in ICC
Enciphered PIN Data	Present if CVM performed is 'enciphered PIN for online verification'
Merchant Category Code	Present for Terminal Type = '2x' if Merchant Identifier or Terminal Identifier does not implicitly refer to a single merchant category

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_4_Other_Interfaces_20120607062305603.pdf

8.1.2 Application Cryptogram Algorithm

The method for Application Cryptogram generation takes as input a unique ICC Application Cryptogram Master Key MK_{AC} and the data selected as described in section 8.1.1, and computes the 8-byte Application Cryptogram in the following two steps:

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

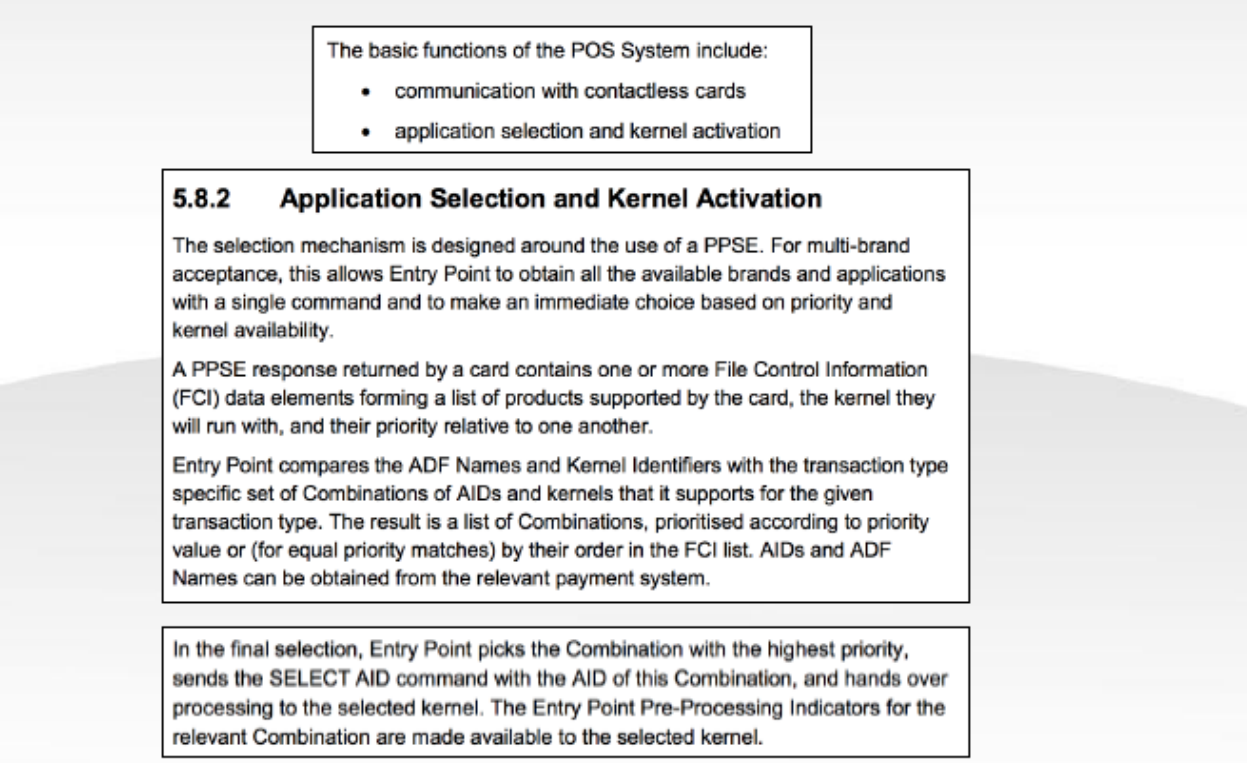
36. Once the mobile wallet is validated, as described below, the transaction is allowed to proceed.

be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication' or simply 'card authentication'.

EMV Integrated Circuit Card Specifications for Payment Systems: Book 3, Application Specification, Version 4.3, November 2011

37. The Accused Instrumentalities of the Citi Defendants infringe at least the claims of the '509 patent, which provide technological solutions and improvements for facilitating payment transactions. Conventional methods for payment transactions, particularly RFID transactions, had problems supporting multiple payment systems. The '509 patent discloses a computer-based system that queries a payment system directory and selects the appropriate payment system. The directory may contain algorithms or rules to allow selection of a payment system based upon payment information, the type of transaction, or the transaction instrument issuer. Payment information may include a proxy account number. Once the payment system is selected, an authorization request with payment information is sent to the payment system. A payment authorization is received by the computer-based system. Systems and methods of the '509 patent, such as these, allow a payment system directory to identify a payment system that is mutually supported and appropriate for a particular transaction.

38. In response to a command from a point of sale terminal, Citi Defendants, via a computer-based system that operates the payment application provisioned by the Citi Defendants, query an onboard payment system directory, as indicated below.



The basic functions of the POS System include:

- communication with contactless cards
- application selection and kernel activation

5.8.2 Application Selection and Kernel Activation

The selection mechanism is designed around the use of a PPSE. For multi-brand acceptance, this allows Entry Point to obtain all the available brands and applications with a single command and to make an immediate choice based on priority and kernel availability.

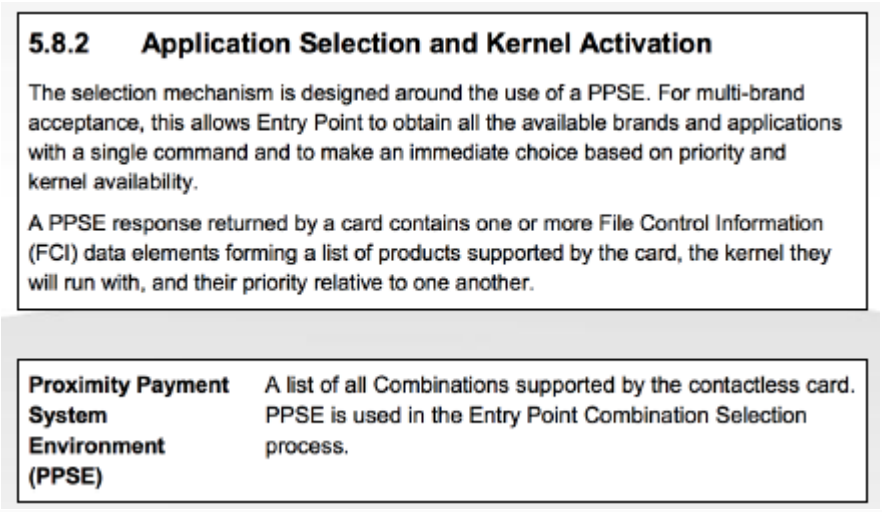
A PPSE response returned by a card contains one or more File Control Information (FCI) data elements forming a list of products supported by the card, the kernel they will run with, and their priority relative to one another.

Entry Point compares the ADF Names and Kernel Identifiers with the transaction type specific set of Combinations of AIDs and kernels that it supports for the given transaction type. The result is a list of Combinations, prioritised according to priority value or (for equal priority matches) by their order in the FCI list. AIDs and ADF Names can be obtained from the relevant payment system.

In the final selection, Entry Point picks the Combination with the highest priority, sends the SELECT AID command with the AID of this Combination, and hands over processing to the selected kernel. The Entry Point Pre-Processing Indicators for the relevant Combination are made available to the selected kernel.

https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf

39. The Citi Defendants' card application stored in a mobile wallet, for example, provides an identification of each supported candidate payment system. A candidate payment system is located for processing a transaction and receives payment information related to the transaction to develop a payment authorization.



5.8.2 Application Selection and Kernel Activation

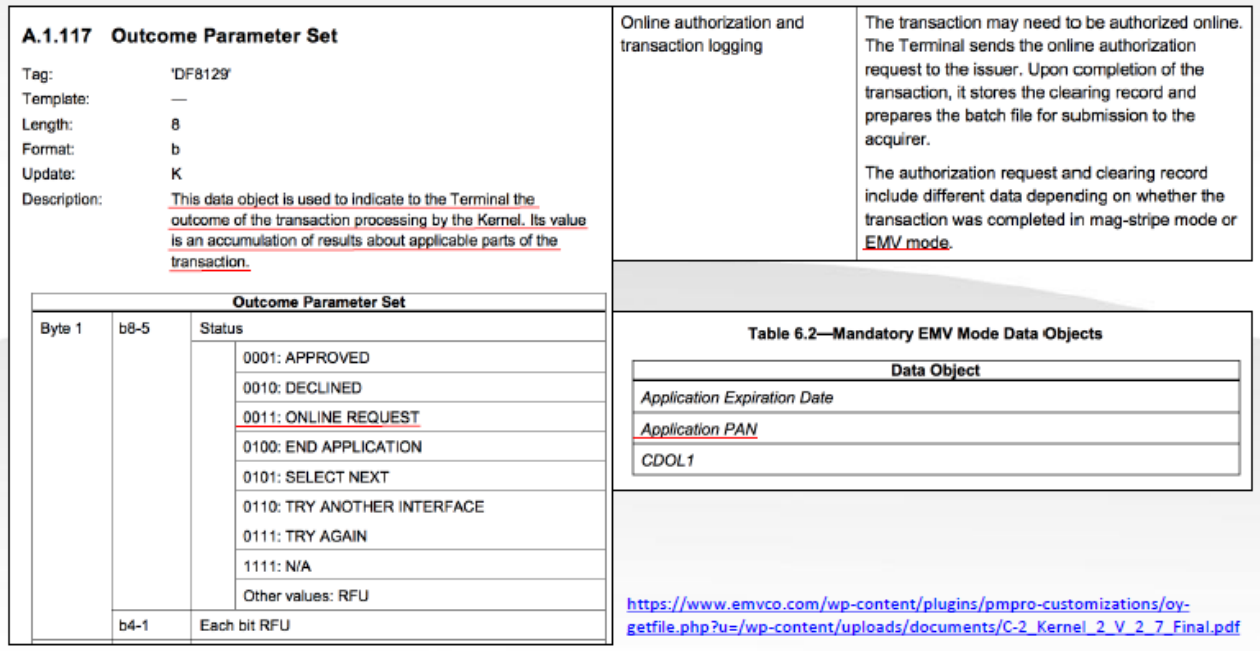
The selection mechanism is designed around the use of a PPSE. For multi-brand acceptance, this allows Entry Point to obtain all the available brands and applications with a single command and to make an immediate choice based on priority and kernel availability.

A PPSE response returned by a card contains one or more File Control Information (FCI) data elements forming a list of products supported by the card, the kernel they will run with, and their priority relative to one another.

Proximity Payment System Environment (PPSE)	A list of all Combinations supported by the contactless card. PPSE is used in the Entry Point Combination Selection process.

https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf

40. As explained below, the Citi Defendants' card application stored in a mobile wallet sends transaction information to the issuer, through the payment system, for authorization.



A.1.117 Outcome Parameter Set

Tag: 'DF8129'
Template: —
Length: 8
Format: b
Update: K
Description: This data object is used to indicate to the Terminal the outcome of the transaction processing by the Kernel. Its value is an accumulation of results about applicable parts of the transaction.

Outcome Parameter Set			
Byte 1	b8-5	Status	
			0001: APPROVED
			0010: DECLINED
			0011: ONLINE REQUEST
			0100: END APPLICATION
			0101: SELECT NEXT
			0110: TRY ANOTHER INTERFACE
			0111: TRY AGAIN
			1111: N/A
			Other values: RFU
	b4-1	Each bit RFU	

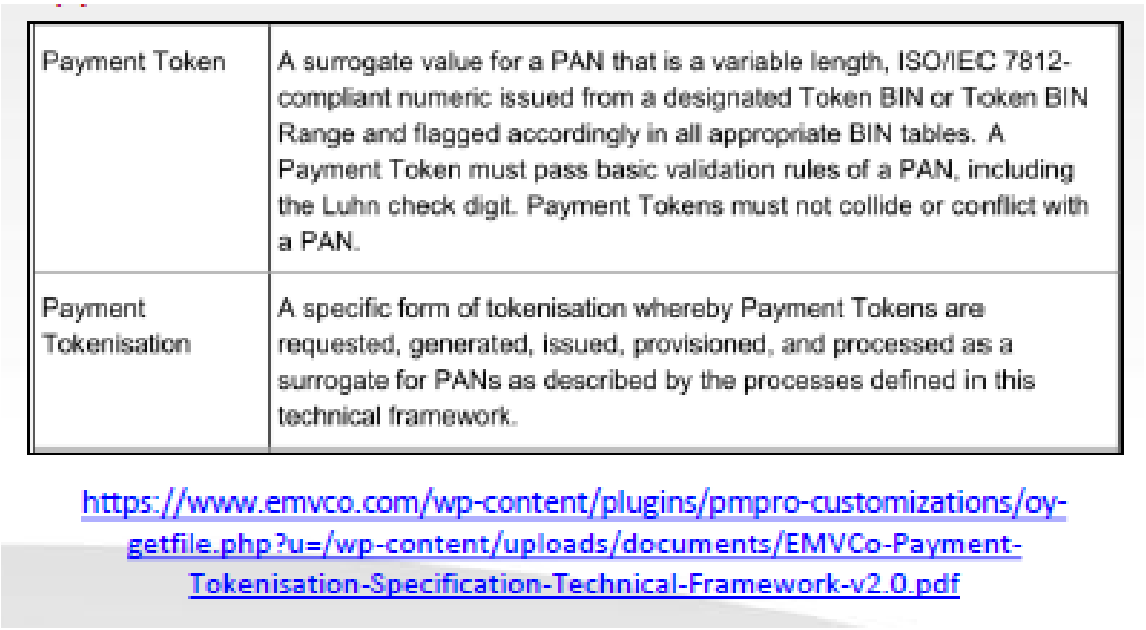
Online authorization and transaction logging	The transaction may need to be authorized online. The Terminal sends the online authorization request to the issuer. Upon completion of the transaction, it stores the clearing record and prepares the batch file for submission to the acquirer. The authorization request and clearing record include different data depending on whether the transaction was completed in mag-stripe mode or EMV mode.

Table 6.2—Mandatory EMV Mode Data Objects

Data Object
Application Expiration Date
Application PAN
CDOL1

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf

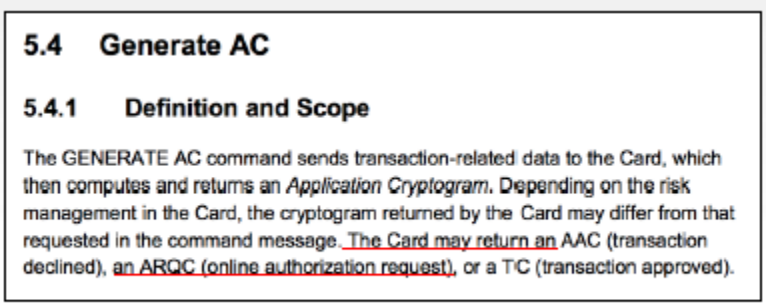
41. As explained below, the Citi Defendants store a token, in place of a primary account number ("PAN"), in a mobile wallet application, for example.



Payment Token	A surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric issued from a designated Token BIN or Token BIN Range and flagged accordingly in all appropriate BIN tables. A Payment Token must pass basic validation rules of a PAN, including the Luhn check digit. Payment Tokens must not collide or conflict with a PAN.
Payment Tokenisation	A specific form of tokenisation whereby Payment Tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs as described by the processes defined in this technical framework.

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0.pdf

42. The Citi Defendants' card application stored in a mobile wallet transmits a payment authorization request, related to the transaction, through the payment system for processing. As indicated below, the card application receives the issuer authorization through the payment system.



5.4 Generate AC

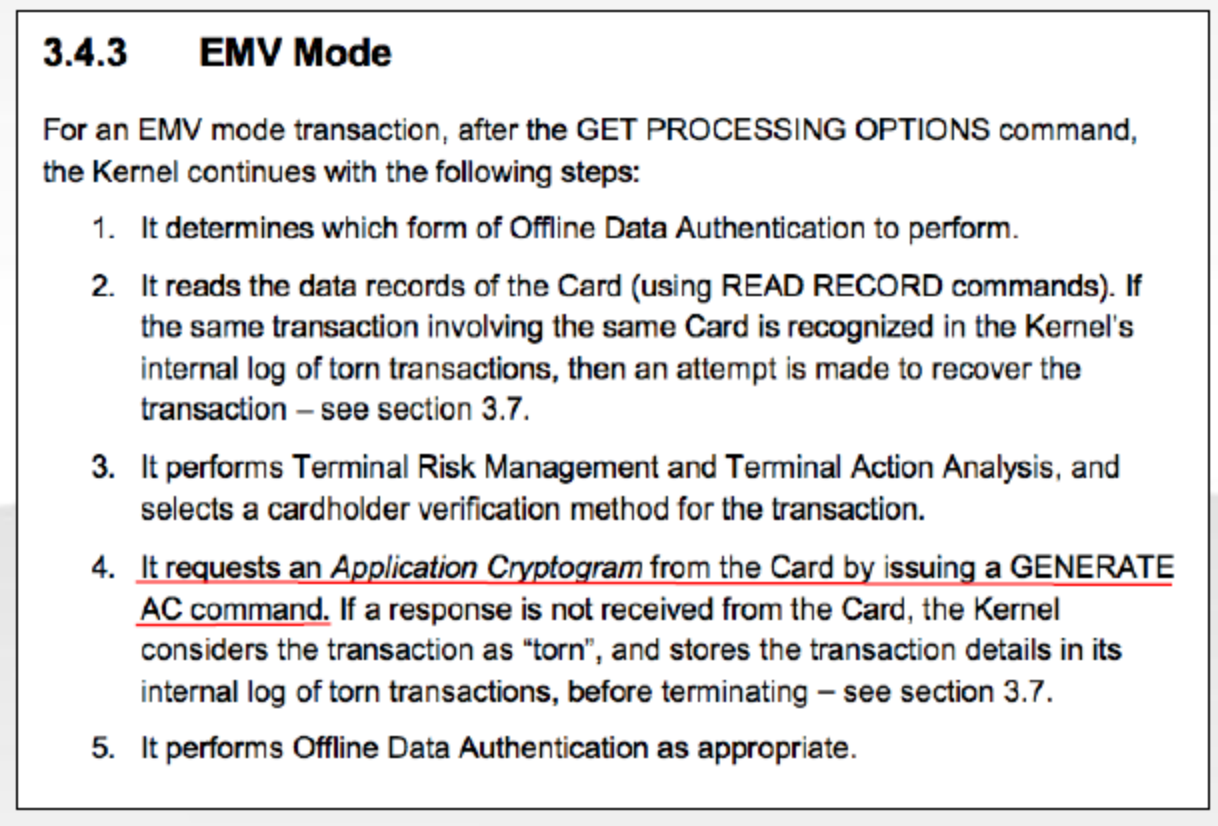
5.4.1 Definition and Scope

The GENERATE AC command sends transaction-related data to the Card, which then computes and returns an *Application Cryptogram*. Depending on the risk management in the Card, the cryptogram returned by the Card may differ from that requested in the command message. The Card may return an AAC (transaction declined), an ARQC (online authorization request), or a TC (transaction approved).

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf

43. The Accused Instrumentalities of the Citi Defendants infringe at least the claims of the '369 patent, which provide technological solutions and improvements for facilitating payment transactions. Conventional methods for payment transactions, particularly RFID transactions, had problems supporting multiple payment systems. The '369 patent provides systems and methods that can be used by smartcards, including contactless credit and debit cards and mobile wallets. The smartcard receives a payment request for a transaction. The smartcard determines a first payment system for processing the transaction, where such determination includes a query for payment directory information stored on the smartcard. The smartcard transmits to a point of sale device (POS) an identification of the payment system. Systems and methods of the '369 patent, such as these, allow a payment system directory to identify a payment system that is mutually supported and appropriate for a particular transaction.

44. The Citi Defendants provide contactless credit and debit cards and mobile wallet payment applications configured with smartcards that receive payment requests from POS terminals. For example, in a Kernel 2 application (i.e., a MasterCard transaction) a card responds to an Application Cryptogram (AC) command from the terminal, as indicated below.



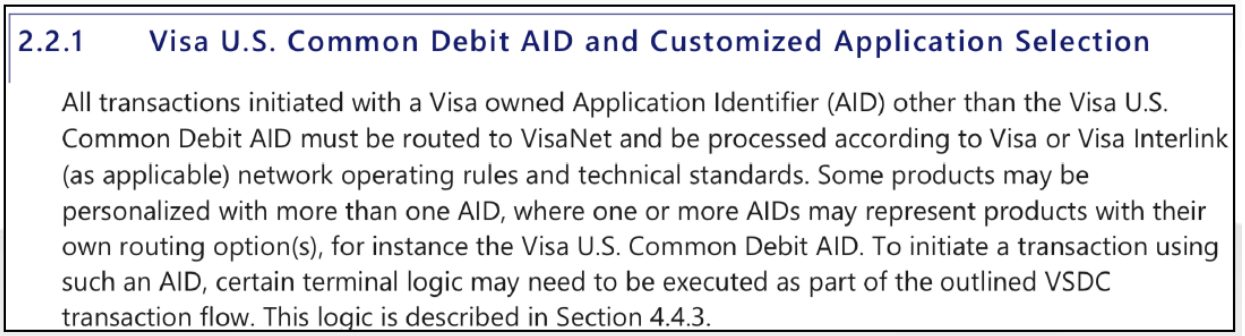
3.4.3 EMV Mode

For an EMV mode transaction, after the GET PROCESSING OPTIONS command, the Kernel continues with the following steps:

1. It determines which form of Offline Data Authentication to perform.
2. It reads the data records of the Card (using READ RECORD commands). If the same transaction involving the same Card is recognized in the Kernel's internal log of torn transactions, then an attempt is made to recover the transaction – see section 3.7.
3. It performs Terminal Risk Management and Terminal Action Analysis, and selects a cardholder verification method for the transaction.
4. It requests an *Application Cryptogram* from the Card by issuing a GENERATE AC command. If a response is not received from the Card, the Kernel considers the transaction as "torn", and stores the transaction details in its internal log of torn transactions, before terminating – see section 3.7.
5. It performs Offline Data Authentication as appropriate.

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf

45. The smartcard provided by Citi Defendants in contactless cards and mobile wallets query a payment system directory in response to a command from the POS terminal. The contactless card or mobile wallet, via the smartcard, will transmit an identification of each supported payment system. The identification is usable by the POS terminal. As shown below, a POS device may support one or more applications (payment systems), where each payment system is associated with an Application Identifier (AID), e.g., Visa AIDs are routed through VisaNet—the payment system.



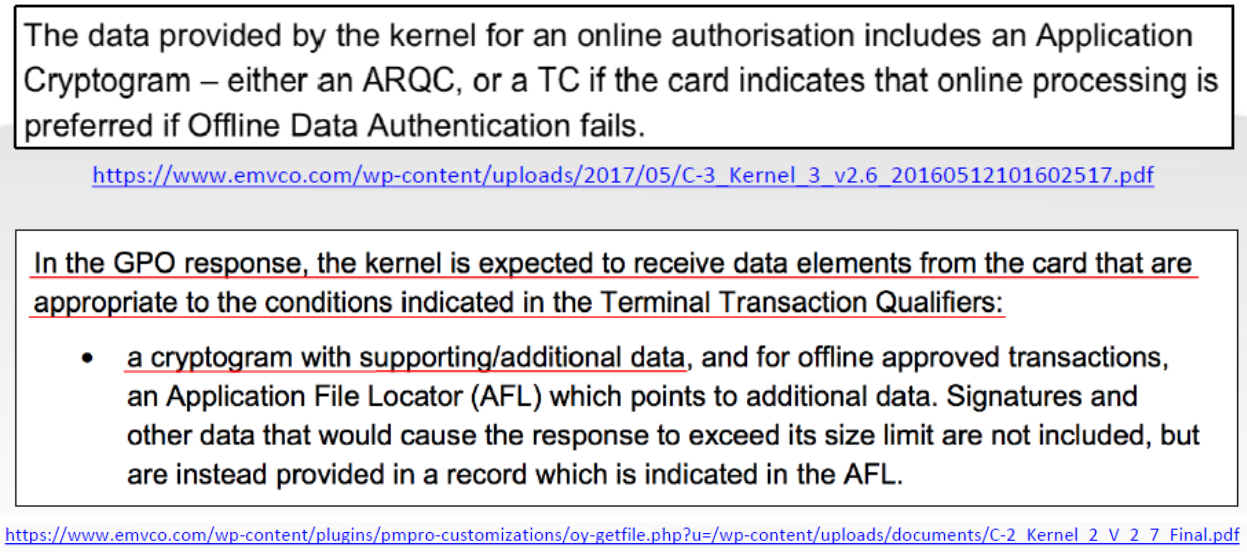
2.2.1 Visa U.S. Common Debit AID and Customized Application Selection

All transactions initiated with a Visa owned Application Identifier (AID) other than the Visa U.S. Common Debit AID must be routed to VisaNet and be processed according to Visa or Visa Interlink (as applicable) network operating rules and technical standards. Some products may be personalized with more than one AID, where one or more AIDs may represent products with their own routing option(s), for instance the Visa U.S. Common Debit AID. To initiate a transaction using such an AID, certain terminal logic may need to be executed as part of the outlined VSDC transaction flow. This logic is described in Section 4.4.3.

https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/docs/visa-emv-merchant-aig.pdf

46. The Accused Instrumentalities of the Citi Defendants infringe at least claims of the '181 patent, which provide technological solutions and improvements for payment system technologies, including methods for authorizing RFID transaction devices. Conventional methods for securing RFID transactions required that during a transaction, the device user provide a secondary form of identification. Such methods, however, increased the time to complete the transaction, which created a barrier to adoption of the methods by users. In at least exemplary embodiment, the '181 patent addresses the need for securing RFID transactions by generating a unique tag comprising a counter value, a device identifier, and a randomly generated number. After generating this tag and receiving verification, the device increments the counter value and authorizes a transaction. The methods from the '181 patent ensure that transactions devices are used for intended transactions and provide security for consumers, without increasing the time to complete the transactions and without device user intervention.

47. The Citi Defendants, for example, support mobile payments that utilize mobile wallets, such as Google Pay and Samsung Pay. These mobile wallets conform to EMV standards. As described below with respect to the mobile wallet Google Pay and as one example, the Citi Defendants provision mobile wallets with their own credentials and EMV applications. This card application generates an Application Cryptogram for authentication. The Application Cryptogram for online authorization (ARQC) consists of an unpredictable number from an RFID terminal.



The data provided by the kernel for an online authorisation includes an Application Cryptogram – either an ARQC, or a TC if the card indicates that online processing is preferred if Offline Data Authentication fails.

https://www.emvco.com/wp-content/uploads/2017/05/C-3_Kernel_3_v2.6_20160512101602517.pdf

In the GPO response, the kernel is expected to receive data elements from the card that are appropriate to the conditions indicated in the Terminal Transaction Qualifiers:

- a cryptogram with supporting/additional data, and for offline approved transactions, an Application File Locator (AFL) which points to additional data. Signatures and other data that would cause the response to exceed its size limit are not included, but are instead provided in a record which is indicated in the AFL.

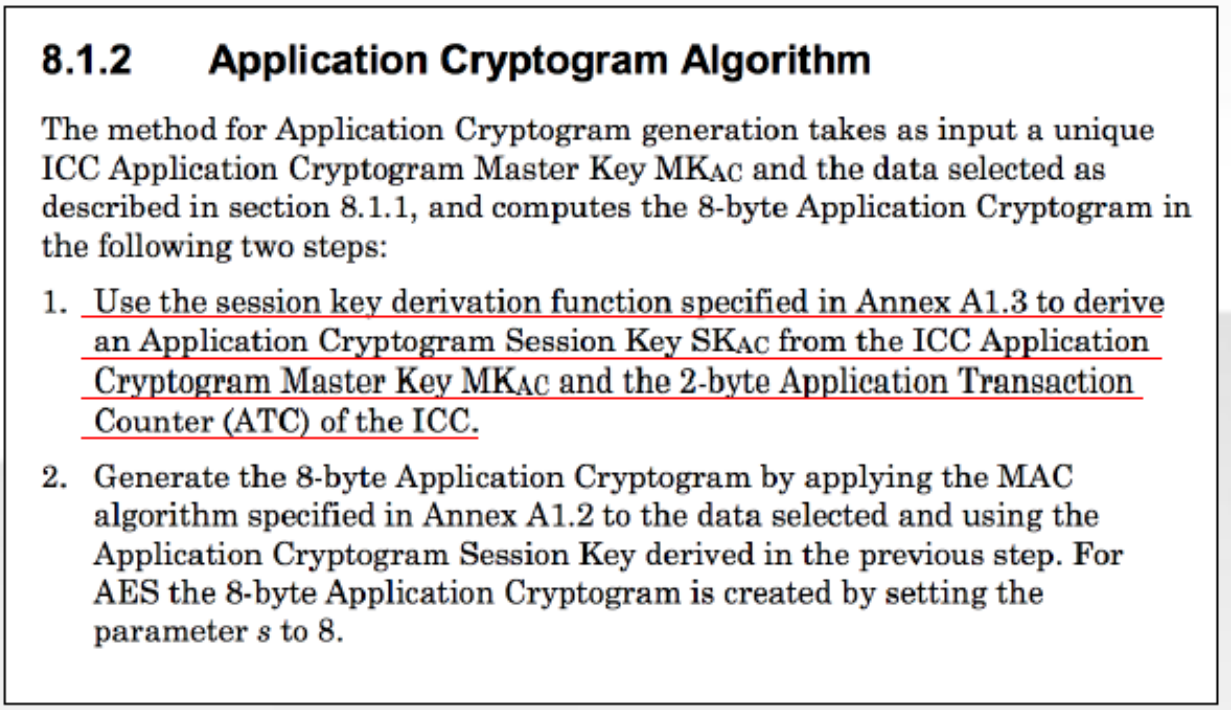
https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf

48. The Application Cryptogram is encrypted using a Limited use Key (LUK) from the terminal, as indicated below. The LUK includes the Application Transaction Counter (ATC) value at the time the LUK was generated, and an Application Cryptogram Master Key, which uniquely identifies the RFID terminal.

limited-use key

Basically, the limited-use key (LUK) - also called the **single-use key** (SUK) - is the password that joins the **token** with the actual card number, and, without it, the token can not be validated by the token service provider and matched to the actual card number to successfully complete a purchase. No other master key data is stored on the device. If the device is rebooted and has no network connection, it cannot decrypt LUKs / SUKs and, therefore, cannot be used for in-store transactions.

https://support.google.com/pay/merchants/answer/7151225?hl=en



8.1.2 Application Cryptogram Algorithm

The method for Application Cryptogram generation takes as input a unique ICC Application Cryptogram Master Key MK_{AC} and the data selected as described in section 8.1.1, and computes the 8-byte Application Cryptogram in the following two steps:

1. Use the session key derivation function specified in Annex A1.3 to derive an Application Cryptogram Session Key SK_{AC} from the ICC Application Cryptogram Master Key MK_{AC} and the 2-byte Application Transaction Counter (ATC) of the ICC.
2. Generate the 8-byte Application Cryptogram by applying the MAC algorithm specified in Annex A1.2 to the data selected and using the Application Cryptogram Session Key derived in the previous step. For AES the 8-byte Application Cryptogram is created by setting the parameter *s* to 8.

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

49. The microchip card application of the Citi Defendants transmits the ARQC to a RFID terminal, as described below, and the ATC is incremented to indicate whether thresholds of the LUK have been exceeded or not.

5.4 Generate AC

5.4.1 Definition and Scope

The GENERATE AC command sends transaction-related data to the Card, which then computes and returns an *Application Cryptogram*. Depending on the risk management in the Card, the cryptogram returned by the Card may differ from that requested in the command message. The Card may return an AAC (transaction declined), an ARQC (online authorization request), or a TC (transaction approved).

Online authorization and transaction logging	The transaction may need to be authorized online. The Terminal sends the online authorization request to the issuer. Upon completion of the transaction, it stores the clearing record and prepares the batch file for submission to the acquirer. The authorization request and clearing record include different data depending on whether the transaction was completed in mag-stripe mode or EMV mode.

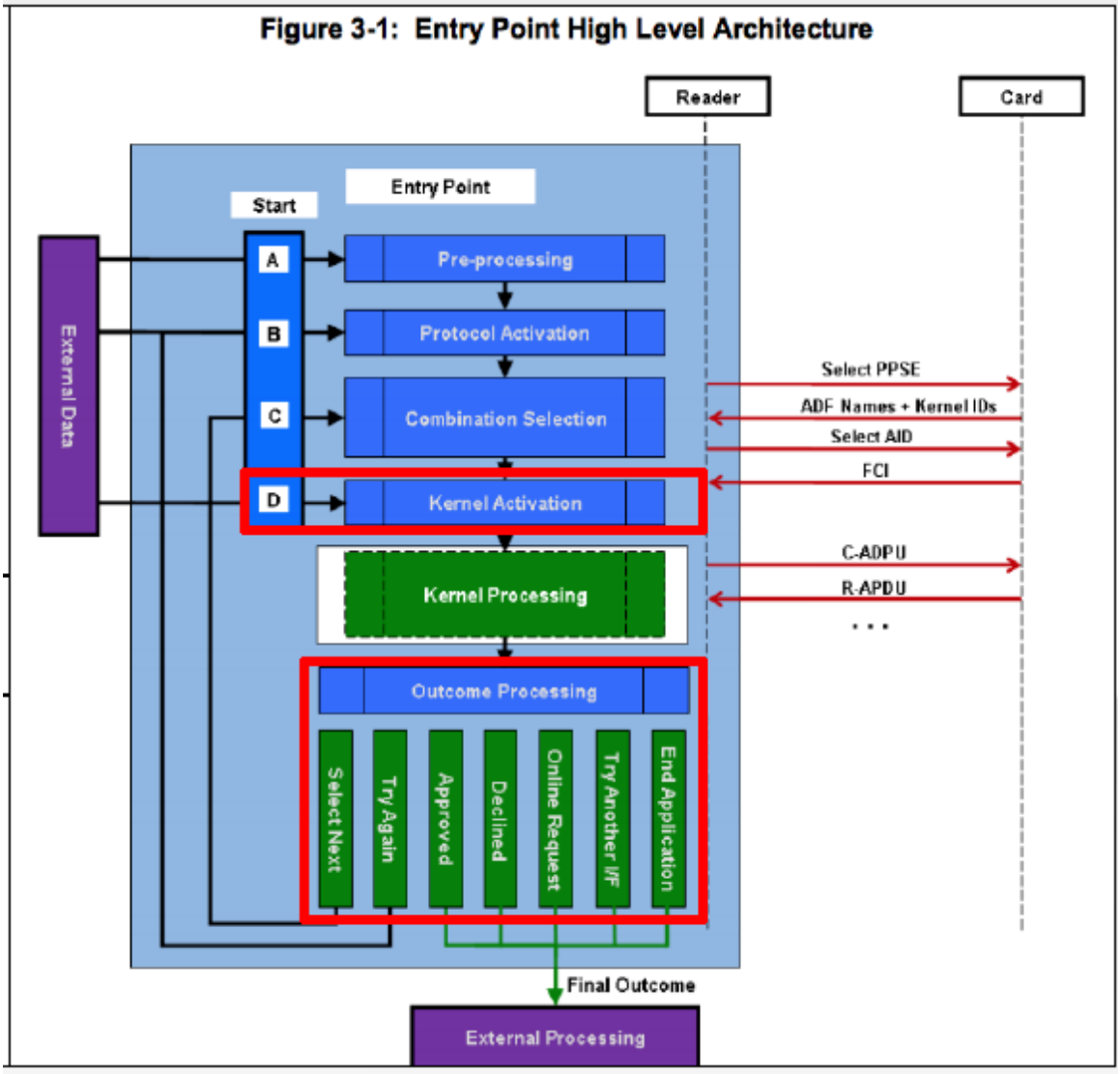
2.4.7 Online Processing

Online Processing is implemented for EMV mode readers supporting online transactions. The kernel indicates the need for online processing by means of the Outcome and parameters.

The data provided by the kernel for an online authorisation includes an Application Cryptogram – either an ARQC, or a TC if the card indicates that online processing is preferred if Offline Data Authentication fails.

https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-2_Kernel_2_V_2_7_Final.pdf
https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/C-3_Kernel_3_V_2_7_Final.pdf

50. The RFID transaction is authorized once the Citi Defendants verify the LUK and the ARQC.

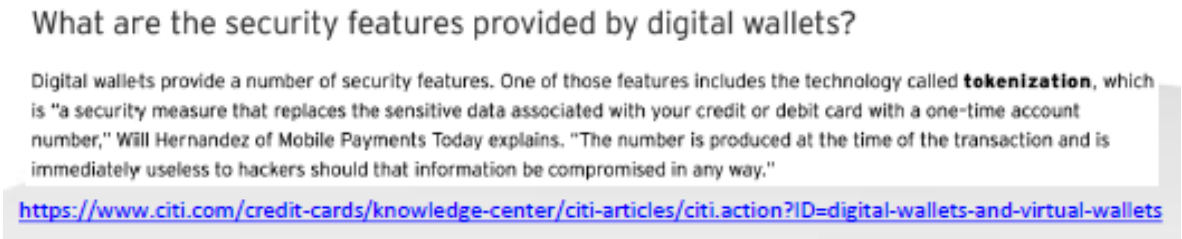


https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf
https://www.emvco.com/wp-content/uploads/2017/05/BookB_Entry_Point_Specification_v2_6_20160809023257319.pdf

51. The Accused Instrumentalities of the Citi Defendants infringe at least the claims of the '985 patent, which provide methods and systems for authorizing payment transactions for customers with more than one transaction instrument representing a single transaction account. In the '985 patent, customer-level transaction data may be determined to be common to more than one

instrument, and such data may be analyzed in order to authorize a payment transaction. Data elements may be verified across multiple records for an individual customer. One advantage of such verification is that it improves the accuracy of transaction risk calculations, for example, by reducing the probability of errors during fraud detection. Other advantages include providing merchants with comparison results at the data element level to assist in a decision-making process. In at least one exemplary embodiment of the '985 patent, a computer system may receive an authorization request from a merchant for a transaction. Such transaction may be initiated by using a transaction instrument corresponding to a user. The computer system may determine a second transaction instrument corresponding to the user. To authorize the transaction, the computer system may analyze transaction data that corresponds to transaction data associated with the second transaction. The '985 patent allows for increased security and confidence during a transaction and reduces the number of incorrectly declined transactions due to authorization errors as well as providing an increase in customer satisfaction.

52. The Citi Defendants infringe the '985 patent by enabling and conducting mobile payments that use the Citi's Defendants EMV payment applications in conjunction with mobile wallets, such as Google Pay and Samsung Pay. The Citi Defendants create virtual account numbers, referred to as tokens in the mobile wallet context, for provisioning to mobile wallets and initiating payment card transactions. Citi credit card transactions made online by consumers may also utilize virtual account numbers, as shown below.



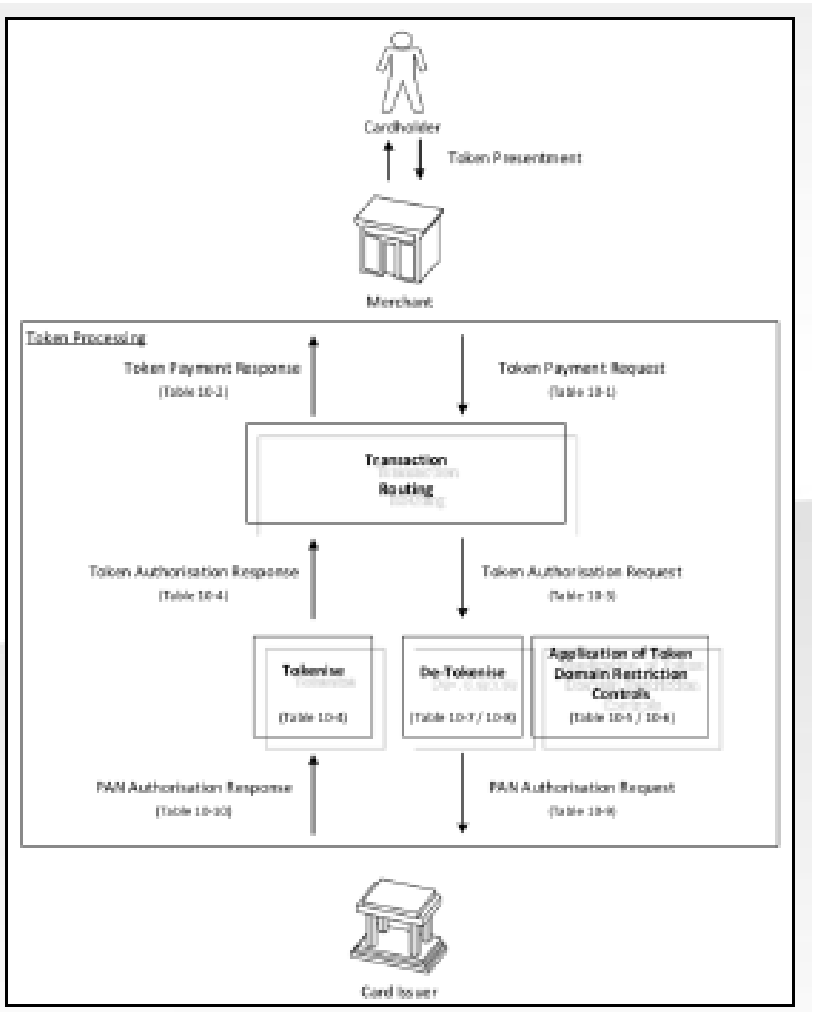
Included with Select Citi® Cards

Citi helps make my credit card number virtually impossible to steal by generating a random Citi card number that I can use while shopping online.

When shopping online or by mail order, you can use a randomly generated Citi card Virtual Account Number instead of your real account number. Simply click Enroll in/Get below to begin using Virtual Account Numbers.

https://www.cardbenefits.citi.com/Products/Virtual-Account-Numbers

53. As shown below, tokenized account numbers (i.e., a first transaction instrument) are sent to the Citi Defendants for de-tokenization and authorization.



Token Payment Request: includes the request that originates from the point of interaction with the Merchant (such a Terminal, website or application) and the response that provides the results of the authorisation decision

EMV Payment Tokenisation Specification, Technical Framework v2.0, September 2017

54. As explained below, upon receipt of a Payment Token, the Citi Defendants convert the token into the corresponding Citi account number (PAN) of the user.

Payment Token	An existing payment processing field that is passed through the authorisation, capture, clearing, and exception messages in place of the PAN. After De-Tokenisation, the Payment Token is replaced with the underlying PAN. The PAN is then passed to the Card Issuer as part of the PAN Authorisation in this field. The Payment Token may optionally be passed to the Card Issuer as part of the PAN Authorisation using a Payment Network specific Token Processing field.

De-Tokenisation: includes the request and corresponding response processing converting a Payment Token and Token Expiry Date to an underlying PAN and PAN Expiry Date. De-Tokenisation may or may not include the application of Token Domain Restriction Controls

EMV Payment Tokenisation Specification, Technical Framework v2.0, September 2017

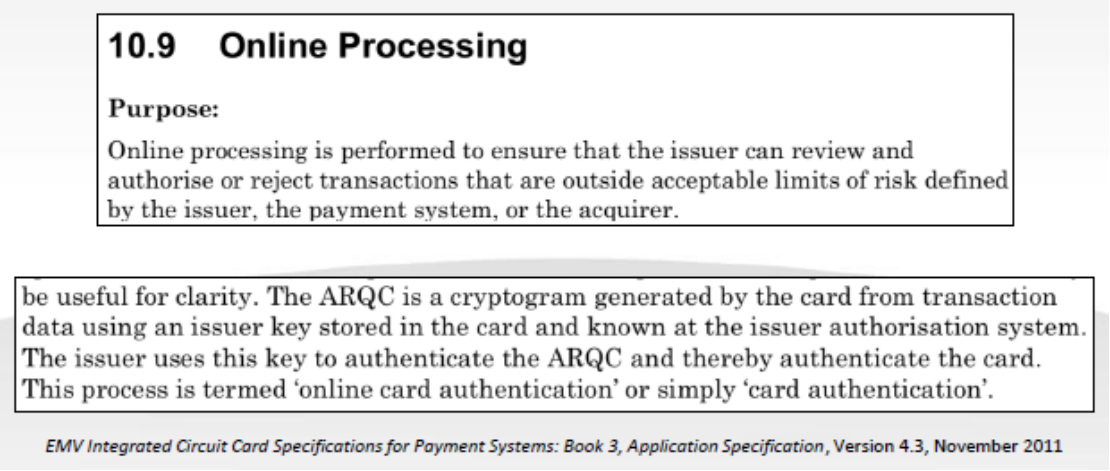
55. The Citi Defendants analyze the transaction data in order to authenticate the transaction, as explained below in relation to an EMV-type transaction.

be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication' or simply 'card authentication'.

EMV Integrated Circuit Card Specifications for Payment Systems: Book 3, Application Specification, Version 4.3, November 2011

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf

56. Based on the analysis for authentication, the Citi Defendants respond to the authorization request with an authorization message.



10.9 Online Processing

Purpose:

Online processing is performed to ensure that the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

be useful for clarity. The ARQC is a cryptogram generated by the card from transaction data using an issuer key stored in the card and known at the issuer authorisation system. The issuer uses this key to authenticate the ARQC and thereby authenticate the card. This process is termed 'online card authentication' or simply 'card authentication'.

EMV Integrated Circuit Card Specifications for Payment Systems: Book 3, Application Specification, Version 4.3, November 2011

57. By utilizing EMV standards, the Accused Instrumentalities include systems and methods for offering, providing, registering, facilitating, maintaining, transacting, authenticating, and processing commercial transactions via credit and debit cards and associated accounts that are covered by the Asserted Patents. Along with the above technology discussion, each respective Count below describes how the Accused Instrumentalities infringe on specific claims of the Asserted Patents.

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,953,671)

58. Plaintiff incorporates paragraphs 1 through 57 herein by reference.

59. Plaintiff is the assignee of the '671 patent, entitled "Methods and Apparatus for Conducting Electronic Transactions," with ownership of all substantial rights in the '671 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

60. The ’671 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’671 patent issued from U.S. Patent Application No. 12/275,924.

61. The Citi Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’671 patent in this District and elsewhere in Texas and the United States.

62. On information and belief, the Citi Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the ’671 patent, which include Citi Defendants’ offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi’s customers, consumers, and clients, as used in mobile payments and digital wallets.

63. Defendant Citigroup directly infringes the ’671 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the ’671 patent to, for example, its alter egos, agents, intermediaries, distributors, customers, subsidiaries, partners, affiliates, clients and/or consumers.

64. Furthermore, Defendant Citigroup directly infringes the ’671 patent through its direct involvement in the activities of its subsidiaries, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc., including by selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Citigroup. On information and belief, the Citi Defendants’ subsidiaries and affiliates conduct activities that constitutes direct infringement of the ’671 patent

under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Citigroup is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. (under both the alter ego and agency theories) because, as an example and on information and belief, Defendant Citigroup, Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. are essentially the same company. Citigroup and Citibank NA have the right and ability to control other subsidiaries' infringing acts (including those activities of Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc.) and receives a direct financial benefit from their infringement.

65. For example, the Citi Defendants infringe claim 1 of the '671 patent via its Accused Instrumentalities that utilize methods that implement EMV standards for mobile or contactless payments. The Citi Defendants provide, for example, to consumers payment cards, such as credit and debit cards, that support mobile or contactless payments that conform to the EMV standards. The Citi Defendants' mobile payments can be facilitated by using mobile wallets such as Google Pay and Samsung Pay. The Citi Defendants, as the payment card issuer, direct and control, including via their alter egos, agents, affiliates, partners, and subsidiaries, the operation of these mobile or contactless payments conducted using Citi issued payment cards, including the provisioning, authenticating, and authorizing of mobile payment wallets and transactions therein.

66. The Accused Instrumentalities implement the method of claim 1 of the '671 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused

Instrumentalities include a method that implements the steps of forwarding, by a computer-based system for conducting a transaction, a challenge to an intelligent token of a client, wherein said intelligent token generates a challenge response, and wherein said computer-based system comprises a processor and a non-transitory memory; receiving, by said computer-based system, said challenge response; assembling, by said computer-based system, credentials for a transaction in response to verifying said challenge response, wherein said assembled credentials include a key; receiving, by said computer-based system, a request from said client, wherein said request includes at least a portion of said assembled credentials provided to said client; validating, by said computer-based system, said portion of said assembled credentials with said key of said assembled credentials; and, providing, by said computer-based system, access to a transaction service in response to said validating.

67. At a minimum, the Citi Defendants have known of the ’671 patent at least as early as the filing date of this complaint. In addition, the Citi Defendants have known about the ’671 patent since at least April 1, 2019 when, via a letter, Plaintiff initially informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio. On May 6, 2019 via an email to Defendant Citigroup, Plaintiff provided the Citi Defendants with access to a data room containing claim charts for patents in the portfolio. After Plaintiff sought to schedule a call with the Citi Defendants via a series of emails, Plaintiff again sent a letter on April 1, 2020 to the Citi Defendants inviting them to engage in licensing discussions relating to Plaintiff’s patent portfolio, including the ’671 Patent.

68. On information and belief, since at least the above-mentioned date when the Citi Defendants were on notice of their infringement, the Citi Defendants have actively induced, under U.S.C. § 271(b), their distributors, partners, customers, clients, subsidiaries, and/or consumers and

also other payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sale, sell, use, and service the Accused Instrumentalities that include or are made using all of the limitations of one or more claims of the '671 patent to directly infringe one or more claims of the '671 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, the Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '671 patent.

69. On information and belief, the Defendants intend to cause, and have taken affirmative steps to induce, infringement by distributors, partners, customers, clients, subsidiaries, and/or consumers and other payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Citi's Accused Instrumentalities with other mobile payment systems, including with mobile wallet applications; as payment card issuer, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices with the payment applications, generating and installing cryptographic keys, and processing transactions; partnering with retailers and private labels to "co-brand" cards that incentivize use of Citi's payment cards in commerce; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective

buyers; testing Citi's mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., citi.com and citigroup.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities, and/or providing technical support, replacement parts or services for these products and services to purchasers and other consumers, including overdraft protection services, in the United States. *See, e.g., Pay and go, just about anywhere*, CITI, https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-samsung-pay (last visited June 17, 2021) (explaining "How Samsung Pay Works" and "How to Set Up Samsung Pay" and "Where Samsung Pay Works").

70. On information and belief, despite having knowledge of the '671 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '671 patent, the Citi Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. The Citi Defendants' infringing activities relative to the '671 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

71. Plaintiff LPV has been damaged as a result of the Citi Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 8,066,181)

72. Plaintiff incorporates paragraphs 1 through 71 herein by reference.

73. Plaintiff is the assignee of the '181 patent, entitled "RF Transaction Authentication Using a Random Number," with ownership of all substantial rights in the '181 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

74. The '181 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '181 patent issued from U.S. Patent Application No. US 12/256,310.

75. The Citi Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '181 patent in this District and elsewhere in Texas and the United States.

76. On information and belief, the Citi Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '181 patent, which include Citi Defendants' offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi's customers, consumers, and clients.

77. Defendant Citigroup directly infringes the '181 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '181 patent to, for example, its alter egos, agents, intermediaries, distributors, customers, subsidiaries, partners, affiliates, clients and/or consumers.

78. Furthermore, Defendant Citigroup directly infringes the '181 patent through its direct involvement in the activities of its subsidiaries, including Defendant Citibank NA and other

subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc., including by selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Citigroup. On information and belief, the Citi Defendants' subsidiaries and affiliates conduct activities that constitutes direct infringement of the '181 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Citigroup is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. (under both the alter ego and agency theories) because, as an example and on information and belief, Defendant Citigroup, Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. are essentially the same company. Citigroup and Citibank NA have the right and ability to control other subsidiaries' infringing acts (including those activities of Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc.) and receives a direct financial benefit from their infringement.

79. For example, the Citi Defendants infringe claim 1 of the '181 patent via its Accused Instrumentalities that utilize methods that implement EMV standards for mobile or contactless payments. The Citi Defendants provide, for example, to consumers payment cards, such as credit and debit cards, that support mobile or contactless payments that conform to the EMV standards. The Citi Defendants' mobile payments can be facilitated by using mobile wallets such as Google Pay and Samsung Pay, or such contactless payments can be facilitated by using microchips embedded on the physical credit or debit card of Citi. The Citi Defendants, as the payment card

issuer, direct and control, including via their alter egos, agents, affiliates, partners, and subsidiaries, the operation of these mobile or contactless payments conducted using Citi issued payment cards.

80. The Accused Instrumentalities implement the method of claim 1 of the '181 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Instrumentalities include a method that implements the steps of generating, in a radio frequency identification (RFID) transaction device, an RFID transaction device authentication tag using a random number, a transaction device identifier, and a counter value, wherein the random number is received from an RFID reader; transmitting the RFID transaction device authentication tag to the RFID reader; and incrementing the counter value; wherein an RFID transaction is authorized in response to verification of the RFID transaction device authentication tag.

81. At a minimum, the Citi Defendants have known of the '181 patent at least as early as the filing date of this complaint. In addition, the Citi Defendants have known about the '181 patent since at least April 1, 2019 when, via a letter, Plaintiff initially informed Defendants of Plaintiff's acquisition of the American Express patent portfolio. On May 6, 2019 via an email to Defendant Citigroup, Plaintiff provided the Citi Defendants with access to a data room containing claim charts for patents in the portfolio. After Plaintiff sought to schedule a call with the Citi Defendants via a series of emails, Plaintiff again sent a letter on April 1, 2020 to the Citi Defendants inviting them to engage in licensing discussions relating to Plaintiff's patent portfolio, including the '181 Patent.

82. On information and belief, since at least the above-mentioned date when the Citi Defendants were on notice of their infringement, the Citi Defendants have actively induced, under U.S.C. § 271(b), their distributors, partners, customers, clients, subsidiaries, and/or consumers and

also other payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sale, sell, use, and service the Accused Instrumentalities that include or are made using all of the limitations of one or more claims of the '181 patent to directly infringe one or more claims of the '181 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, the Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '181 patent.

83. On information and belief, the Defendants intend to cause, and have taken affirmative steps to induce, infringement by distributors, partners, customers, clients, subsidiaries, and/or consumers and other payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Citi's Accused Instrumentalities with other mobile payment systems, including with mobile wallet applications; as payment card issuer, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices with the payment applications, generating and installing cryptographic keys, and processing transactions; partnering with retailers and private labels to "co-brand" cards that incentivize use of Citi's payment cards in commerce; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective

buyers; testing Citi's mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., citi.com and citigroup.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities, and/or providing technical support, replacement parts or services for these products and services to purchasers and other consumers, including overdraft protection services, in the United States. *See, e.g., Pay and go, just about anywhere*, CITI, https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-samsung-pay (last visited June 17, 2021) (explaining "How Samsung Pay Works" and "How to Set Up Samsung Pay" and "Where Samsung Pay Works").

84. On information and belief, despite having knowledge of the '181 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '181 patent, the Citi Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. The Citi Defendants' infringing activities relative to the '181 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

85. Plaintiff LPV has been damaged as a result of the Citi Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 8,794,509)

86. Plaintiff incorporates paragraphs 1 through 85 herein by reference.

87. Plaintiff is the assignee of the '509 patent, entitled "Systems and Methods for Processing a Payment Authorization Request over Disparate Payment Networks," with ownership of all substantial rights in the '509 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

88. The '509 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '509 patent issued from U.S. Patent Application No. 12/353,109.

89. The Citi Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '509 patent in this District and elsewhere in Texas and the United States.

90. On information and belief, the Citi Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '509 patent, which include Citi Defendants' offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi's customers, consumers, and clients.

91. Defendant Citigroup directly infringes the '509 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '509 patent to, for example, its alter egos, agents, intermediaries, distributors, customers, subsidiaries, partners, affiliates, clients and/or consumers.

92. Furthermore, Defendant Citigroup directly infringes the ’509 patent through its direct involvement in the activities of its subsidiaries, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc., including by selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Citigroup. On information and belief, the Citi Defendants’ subsidiaries and affiliates conduct activities that constitutes direct infringement of the ’509 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Citigroup is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. (under both the alter ego and agency theories) because, as an example and on information and belief, Defendant Citigroup, Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. are essentially the same company. Citigroup and Citibank NA have the right and ability to control other subsidiaries’ infringing acts (including those activities of Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc.) and receives a direct financial benefit from their infringement.

93. For example, the Citi Defendants infringe claim 1 of the ’509 patent via its Accused Instrumentalities that utilize EMV standards for mobile or contactless payments. The Citi Defendants provide, for example, to consumers payment cards, such as credit and debit cards, that support mobile or contactless payments that conform to the EMV standards. The Citi Defendants’ mobile payments can be facilitated by using mobile wallets such as Google Pay and Samsung Pay. The Citi Defendants, as the payment card issuer, direct and control, including via their alter egos,

agents, affiliates, partners, and subsidiaries, the operation of these mobile or contactless payments conducted using Citi issued payment cards, including by provisioning the mobile devices with EMV-compliant card payment applications.

94. The Accused Instrumentalities implement the method of claim 1 of the '509 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Instrumentalities include a method implementing the steps of querying, by a computer-based system configured to facilitate a transaction, a payment system directory, wherein said payment system directory communicates with said computer-based system, and wherein said payment system directory comprises information regarding a plurality of candidate payment systems, and wherein said payment system directory locates a candidate payment system for processing at least a portion of said transaction, wherein said candidate payment system receives payment information related to said transaction for developing a payment authorization, and wherein said payment information includes a proxy account number; transmitting, by said computer-based system, a payment authorization request related to said transaction to said candidate payment system; and receiving, by said computer-based system, said payment authorization from said candidate payment system.

95. At a minimum, the Citi Defendants have known of the '509 patent at least as early as the filing date of this complaint. In addition, the Citi Defendants have known about the '509 patent since at least April 1, 2019 when, via a letter, Plaintiff initially informed Defendants of Plaintiff's acquisition of the American Express patent portfolio. On May 6, 2019 via an email to Defendant Citigroup, Plaintiff provided the Citi Defendants with access to a data room containing claim charts, including for the '509 patent. After Plaintiff sought to schedule a call with the Citi Defendants via a series of emails, Plaintiff again sent a letter on April 1, 2020 to the Citi Defendants

inviting them to engage in licensing discussions relating to Plaintiff's patent portfolio, including the '509 Patent.

96. On information and belief, since at least the above-mentioned date when the Citi Defendants were on notice of their infringement, the Citi Defendants have actively induced, under U.S.C. § 271(b), their distributors, partners, customers, clients, subsidiaries, and/or consumers and also other payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sale, sell, use, and service the Accused Instrumentalities that include or are made using all of the limitations of one or more claims of the '509 patent to directly infringe one or more claims of the '509 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, the Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '509 patent.

97. On information and belief, the Defendants intend to cause, and have taken affirmative steps to induce, infringement by distributors, partners, customers, clients, subsidiaries, and/or consumers and other payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Citi's Accused Instrumentalities with other mobile payment systems, including with mobile wallet applications; as payment card issuer, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices with the payment applications, generating and installing cryptographic keys, and processing transactions;

partnering with retailers and private labels to "co-brand" cards that incentivize use of Citi's payment cards in commerce; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Citi's mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., citi.com and citigroup.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities, and/or providing technical support, replacement parts or services for these products and services to purchasers and other consumers, including overdraft protection services, in the United States. *See, e.g., Pay and go, just about anywhere*, CITI, https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-samsung-pay (last visited June 17, 2021) (explaining "How Samsung Pay Works" and "How to Set Up Samsung Pay" and "Where Samsung Pay Works").

98. On information and belief, despite having knowledge of the '509 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '509 patent, the Citi Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. The Citi Defendants' infringing activities relative to the '509 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

99. Plaintiff LPV has been damaged as a result of the Citi Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV

(INFRINGEMENT OF U.S. PATENT NO. 8,851,369)

100. Plaintiff incorporates paragraphs 1 through 99 herein by reference.

101. Plaintiff is the assignee of the '369 patent, entitled "Systems and Methods for Transaction Processing Using a Smartcard," with ownership of all substantial rights in the '369 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

102. The '369 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '369 patent issued from U.S. Patent Application No. 12/505,164.

103. The Citi Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '369 patent in this District and elsewhere in Texas and the United States.

104. On information and belief, the Citi Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '369 patent, which include Citi Defendants' offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi's customers, consumers, and clients.

105. Defendant Citigroup directly infringes the ’369 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the ’369 patent to, for example, its alter egos, agents, intermediaries, distributors, customers, subsidiaries, partners, affiliates, clients and/or consumers.

106. Furthermore, Defendant Citigroup directly infringes the ’369 patent through its direct involvement in the activities of its subsidiaries, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc., including by selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Citigroup. On information and belief, the Citi Defendants’ subsidiaries and affiliates conduct activities that constitutes direct infringement of the ’369 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Citigroup is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. (under both the alter ego and agency theories) because, as an example and on information and belief, Defendant Citigroup, Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. are essentially the same company. Citigroup and Citibank NA have the right and ability to control other subsidiaries’ infringing acts (including those activities of Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc.) and receives a direct financial benefit from their infringement.

107. For example, the Citi Defendants infringe claim 1 of the ’369 patent via its Accused Instrumentalities that implement EMV standards for mobile or contactless payments. The Citi Defendants provide, for example, to consumers payment cards, such as credit and debit cards, that support mobile or contactless payments that conform to the EMV standards. The Citi Defendants’ mobile payments can be facilitated by using mobile wallets such as Google Pay and Samsung Pay, or such contactless payments can be facilitated by using microchips embedded on the physical credit or debit card of Citi. The Citi Defendants, as the payment card issuer, perform and/or direct and control, including via their alter egos, agents, affiliates, partners, and subsidiaries, the operation of these mobile or contactless payments conducted using Citi issued payment cards.

108. The Accused Instrumentalities implement the method of claim 1 of the ’369 patent. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff’s allegations that each of those limitations are met. For example, the Accused Instrumentalities include a method implementing the steps of receiving, at a smartcard, a payment request for a transaction; determining, by the smartcard, a first payment system for processing at least a portion of the transaction, wherein said determining includes the smartcard querying payment directory information stored on the smartcard; and transmitting, by the smartcard, an identification of the first payment system to a point of service (POS) device, wherein the identification is usable by the POS device to transmit a first authorization request related to at least a portion of the transaction to the first payment system.

109. At a minimum, the Citi Defendants have known of the ’369 patent at least as early as the filing date of this complaint. In addition, the Citi Defendants have known about the ’369 patent since at least April 1, 2019 when, via a letter, Plaintiff initially informed Defendants of Plaintiff’s acquisition of the American Express patent portfolio. On May 6, 2019 via an email to

Defendant Citigroup, Plaintiff provided the Citi Defendants with access to a data room containing claim charts, including for the '369 patent. After Plaintiff sought to schedule a call with the Citi Defendants via a series of emails, Plaintiff again sent a letter on April 1, 2020 to the Citi Defendants inviting them to engage in licensing discussions relating to Plaintiff's patent portfolio, including the '369 patent.

110. On information and belief, since at least the above-mentioned date when the Citi Defendants were on notice of their infringement, the Citi Defendant have actively induced, under U.S.C. § 271(b), their distributors, partners, customers, clients, subsidiaries, and/or consumers and also other payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sale, sell, use, and service the Accused Instrumentalities that include or are made using all of the limitations of one or more claims of the '369 patent to directly infringe one or more claims of the '369 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, the Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '369 patent.

111. On information and belief, the Defendants intend to cause, and have taken affirmative steps to induce, infringement by distributors, partners, customers, clients, subsidiaries, and/or consumers and other payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment and contactless payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Citi's Accused Instrumentalities with other mobile payment systems, including with mobile wallet applications; as payment card issuer, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile

wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices with the payment applications, generating and installing cryptographic keys, and processing transactions; partnering with retailers and private labels to "co-brand" cards that incentivize use of Citi's payment cards in commerce; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Citi's mobile and contactless payment features in the Accused Instrumentalities; providing websites (e.g., citi.com and citigroup.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities, and/or providing technical support, replacement parts or services for these products and services to purchasers and other consumers, including overdraft protection services, in the United States. *See, e.g.*, *See Citi Credit Card Benefits*, CITI, https://www.cardbenefits.citi.com/Products/Contactless-Card (last visited June 15, 2021) ("Make everyday purchases quickly and safely with just a tap of your contactless-chip enable card."); *Pay and go, just about anywhere*, CITI, https://www.citi.com/credit-cards/creditcards/citi.action?ID=citi-samsung-pay (last visited June 17, 2021) (explaining "How Samsung Pay Works" and "How to Set Up Samsung Pay" and "Where Samsung Pay Works").

112. On information and belief, despite having knowledge of the '369 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '369 patent, the Citi Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. The Citi Defendants' infringing activities relative to the '369 patent

have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

113. Plaintiff LPV has been damaged as a result of the Citi Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT V

(INFRINGEMENT OF U.S. PATENT NO. 9,195,985)

114. Plaintiff incorporates paragraphs 1 through 113 herein by reference.

115. Plaintiff is the assignee of the '985 patent, entitled "Method, System, and Computer Program Product for Customer-level Data Verification," with ownership of all substantial rights in the '985 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

116. The '985 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '985 patent issued from U.S. Patent Application No. 11/448,767.

117. The Citi Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '985 patent in this District and elsewhere in Texas and the United States.

118. On information and belief, the Citi Defendants design, develop, manufacture, distribute, sell, offer for sale, and use the Accused Instrumentalities that infringe the '985 patent,

which include Citi Defendants' offering, issuing, providing, registering, facilitating, maintaining, transacting, authenticating, and processing credit card and debit card accounts and related products and services for Citi's customers, consumers, and clients.

119. Defendant Citigroup directly infringes the '985 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using the Accused Instrumentalities, their components, and/or products and processes containing the same that incorporate the fundamental technologies covered by the '985 patent to, for example, its alter egos, agents, intermediaries, distributors, customers, subsidiaries, partners, affiliates, clients and/or consumers.

120. Furthermore, Defendant Citigroup directly infringes the '985 patent through its direct involvement in the activities of its subsidiaries, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc., including by selling, offering for sale, and servicing the Accused Instrumentalities in the U.S. directly for Citigroup. On information and belief, the Citi Defendants' subsidiaries and affiliates conduct activities that constitutes direct infringement of the '985 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or using those Accused Instrumentalities. Citigroup is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. (under both the alter ego and agency theories) because, as an example and on information and belief, Defendant Citigroup, Defendant Citibank NA and other subsidiaries such as Citicorp Credit, Citifinancial Inc., also known as CFNA Receivables (TX) LLC, and Citimortgage Inc. are essentially the same company. Citigroup and Citibank NA have the right and ability to control other subsidiaries' infringing acts (including those activities of Citicorp Credit, Citifinancial Inc., also known as CFNA

Receivables (TX) LLC, and Citimortgage Inc.) and receives a direct financial benefit from their infringement.

121. For example, the Citi Defendants infringe claim 1 of the ’985 patent via its Accused Instrumentalities that utilize methods that implement EMV standards for mobile payments. The Citi Defendants provide, for example, to consumers payment cards, such as credit and debit cards, that support mobile payments that conform to the EMV standards. The Citi Defendants’ mobile payments can be facilitated by using mobile wallets such as Google Pay and Samsung Pay. The Citi Defendants further infringe the ’985 patent via creation and use of virtual account numbers in online shopping transactions conducted with Citi payment cards. The Citi Defendants, as the payment card issuer, perform and/or direct and control, including via their alter egos, agents, affiliates, partners, and subsidiaries, the operation of these mobile conducted using Citi issued payment cards. For example, Citi’s payment applications reside on chip card and mobile devices (including via Host Card Emulation), and such applications perform the steps necessary to accomplish the transaction, including, but not limited to, processing functions, storing information, and performing cryptographic processing.

122. The Accused Instrumentalities implement the method of claim 1. The technology discussion above and the example Accused Instrumentalities provide context for Plaintiff’s allegations that each of those limitations are met. For example, the Accused Instrumentalities practice the following method steps: receiving, by a computer system, an authorization request from a merchant for a transaction, wherein the authorization request indicates that the transaction has been initiated using a first transaction instrument corresponding to a user; based on the authorization request, the computer system determining a second transaction instrument corresponding to the user; the computer system analyzing transaction data for the transaction, wherein the analyzing

includes determining whether the transaction data at least partially corresponds to particular transaction data associated with the second transaction instrument; and based on said analyzing, the computer system transmitting a response to the authorization request to the merchant, wherein the response indicates whether the transaction is authorized.

123. At a minimum, the Citi Defendants have known of the '985 patent at least as early as the filing date of this complaint. In addition, the Citi Defendants have known about the '985 patent since at least April 1, 2019 when, via a letter, Plaintiff initially informed Defendants of Plaintiff's acquisition of the American Express patent portfolio. On May 6, 2019 via an email to Defendant Citigroup, Plaintiff provided the Citi Defendants with access to a data room containing claim charts, including for the '985 patent. After Plaintiff sought to schedule a call with the Citi Defendants via a series of emails, Plaintiff again sent a letter on April 1, 2020 to the Citi Defendants inviting them to engage in licensing discussions relating to Plaintiff's patent portfolio, including the '985 patent.

124. On information and belief, since at least the above-mentioned date when the Citi Defendants were on notice of their infringement, the Citi Defendant have actively induced, under U.S.C. § 271(b), their distributors, partners, customers, clients, subsidiaries, and/or consumers and also other payment platforms (e.g., Samsung and Google mobile wallets) that distribute, purchase, offer to sale, sell, use, and service the Accused Instrumentalities that include or are made using all of the limitations of one or more claims of the '985 patent to directly infringe one or more claims of the '985 patent by using, offering for sale, selling, and/or servicing the Accused Instrumentalities. Since at least the notice provided on the above-mentioned date, the Defendants do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '985 patent.

125. On information and belief, the Defendants intend to cause, and have taken affirmative steps to induce, infringement by distributors, partners, customers, clients, subsidiaries, and/or consumers and other payment platforms used with the Accused Instrumentalities by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Instrumentalities; adopting mobile payment standards and specifications (e.g., the EMV standards) to allow for interoperability of Citi's Accused Instrumentalities with other mobile payment systems, including with mobile wallet applications; as payment card issuer, providing EMV payment applications, related tokens, and virtual account numbers to third-party mobile wallet providers, point of sale terminal providers, merchants (including online and mail order), and users; maintaining such EMV payment applications by personalizing transaction devices with the payment applications, generating and installing cryptographic keys, and processing transactions; partnering with retailers and private labels to "co-brand" cards that incentivize use of Citi's payment cards in commerce; creating and/or maintaining established distribution channels for the Accused Instrumentalities into and within the United States; manufacturing and designing the Accused Instrumentalities in conformity with U.S. laws and regulations; distributing or making available instructions or manuals for these products and related processes to purchasers and prospective buyers; testing Citi's mobile payment features in the Accused Instrumentalities; providing websites (e.g., citi.com and citigroup.com) and mobile applications for clients, customers, and consumers for registering, activating, maintaining, and using (including accessing infringing features of) the Accused Instrumentalities, and/or providing technical support, replacement parts or services for these products and services to purchasers and other consumers, including overdraft protection services, in the United States. *See, e.g.*, *Pay and go, just about anywhere*, CITI, https://www.citi.com/credit-

cards/creditcards/citi.action?ID=citi-samsung-pay (last visited June 17, 2021) (explaining "How Samsung Pay Works" and "How to Set Up Samsung Pay" and "Where Samsung Pay Works").

126. On information and belief, despite having knowledge of the '985 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '985 patent, the Citi Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. The Citi Defendants' infringing activities relative to the '985 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

127. Plaintiff LPV has been damaged as a result of the Citi Defendants' infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to LPV in an amount that adequately compensates LPV for Defendants' infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

128. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

129. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

130. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

131. Plaintiff requests that the Court find in its favor and against Defendants, and that the Court grant Plaintiff the following relief:

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;
3. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
5. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
6. Such other and further relief as the Court deems just and equitable.

Dated: July 8, 2021

Respectfully submitted,

/s _ Terry A. Saad

Terry A. Saad (lead attorney)
Texas Bar No. 24066015
Jeffrey R. Bragalone
Texas Bar No. 02855775
Marcus Benavides
Texas Bar No. 24035574
Hunter S. Palmer
Texas Bar No. 24080748

BRAGALONE OLEJKO SAAD PC
2200 Ross Avenue
Suite 4600W
Dallas, TX 75201
Tel: (214) 785-6670
Fax: (214) 785-6680
tsaad@bosfirm.com
jbragalone@bosfirm.com
mbenavides@bosfirm.com
hpalmer@bosfirm.com

ATTORNEYS FOR PLAINTIFF
LIBERTY PEAK VENTURES, LLC